МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра
на тему

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Виконав студент 2 курсу,
групи ППГЗ-3-24
Спеціальності 281 «Публічне управління та адміністрування»
Освітньо-професійної програми
«Публічна політика та управління в умовах гібридних загроз»
_____ Владлена МУСІЄНКО

Науковий керівник роботи:
кандидат наук з державного управління, доцент
_____ Михайло БІЛОКОНЬ

Харків – 2025

ЗМІСТ

ВСТУП

Актуальність теми. В умовах повномасштабної збройної агресії та глобальних геополітичних зрушень система національної безпеки України проходить через найскладніші випробування за часів своєї незалежності. Ми стали свідками того, як інформаційний простір перетворився на повноцінний театр воєнних дій, де об’єктами ураження стають не лише військові позиції, а й критична інфраструктура, державні реєстри та навіть свідомість громадян. У цій новій реальності інформаційні технології перестали бути просто зручним сервісом чи допоміжним інструментом для чиновників. Сьогодні вони трансформувалися у фундамент виживання держави та ключовий фактор нашої національної стійкості.

Критичний аналіз ситуації показує, що традиційні, жорстко ієрархічні моделі державного управління вже не здатні ефективно реагувати на динаміку сучасних гібридних загроз. Коли ворог застосовує комбіновані атаки – від ракетних ударів по дата-центрах до складних кібероперацій та дезінформаційних кампаній – класична бюрократія виявляється занадто повільною. Виникає гостра потреба у зміні самої філософії публічного адміністрування: переходу від намагання побудувати «глуху оборону» до концепції кіберстійкості, тобто здатності системи функціонувати та відновлюватися навіть під постійним тиском.

Особливої гостроти проблемі надає той факт, що практичне застосування технологій на полі бою – від унікальних систем ситуаційної обізнаності типу Delta до екосистеми оборонних інновацій Brave1 – значно випереджає існуючу нормативно-правову базу та теоретичне осмислення. Ми опинилися в ситуації, коли реальні механізми захисту держави часто працюють не завдяки, а всупереч застарілим адміністративним процедурам. Це створює небезпечний розрив між технологічними можливостями нашого сектору безпеки та

управлінськими рішеннями, які мають їх забезпечувати.

Саме тому дослідження механізмів використання інформаційних технологій у системі національної безпеки є критично важливим для галузі публічного управління. Нам необхідно не лише зафіксувати унікальний український досвід ведення першої у світі кібервійни (як частини спочатку гібридної а потім й повномасштабної війни проти України), а й напрацювати нові, гнучкі моделі взаємодії між державою, приватним ІТ-сектором та громадянським суспільством. Без розв'язання цих управлінських завдань неможливо забезпечити ні ефективний захист сьогодні, ні повноцінну інтеграцію України до євроатлантичної безпекової архітектури в майбутньому.

Метою роботи є обґрунтування теоретико-методологічних засад, аналіз сучасної практики та розробка пропозицій щодо вдосконалення системи публічного управління процесами використання інформаційних технологій для забезпечення національної безпеки України в умовах гібридної війни.

Для досягнення поставленої мети визначено такі *завдання*:

– Розкрити теоретичні засади використання інформаційних технологій у сфері безпеки, виокремивши трансформацію підходів від традиційного кіберзахисту до парадигми кіберстійкості та екосистемного управління.

– Проаналізувати чинне нормативно-правове забезпечення та інституційну структуру управління національною безпекою в ІТ-сфері, зокрема в контексті гармонізації українського законодавства з європейською директивою NIS2.

– Оцінити поточний стан впровадження цифрових інструментів (системи Delta, екосистема Brave1, цифрова мобілізація) у діяльність сектору безпеки і оборони України та виявити ключові управлінські й технічні проблеми.

– Узагальнити передовий міжнародний досвід США, Ізраїлю та Естонії щодо побудови моделей цифрової оборони та визначити можливості його адаптації до українських реалій.

– Обґрунтувати стратегічні напрями оптимізації державної політики, фокусуючись на нових підходах до фінансування оборонних інновацій, кадрового забезпечення та створення «цифрових посольств».

– Розробити шляхи вдосконалення організаційно-правового механізму, зокрема щодо захисту прав інтелектуальної власності у сфері оборонних технологій та переходу до ризик-орієнтованих стандартів сертифікації замість застарілих систем захисту.

Об'єкт дослідження – система публічного управління у сфері національної безпеки України.

Предмет дослідження – Використання інформаційних технологій для забезпечення національної безпеки.

Методи дослідження. Методологічне підґрунтя роботи складає комплекс загальнонаукових та спеціальних методів, застосування яких дозволило досягти поставленої мети та розв'язати визначені завдання:

– системний підхід – використано для розгляду національної безпеки не як статичної структури, а як динамічної екосистеми, де інформаційні технології забезпечують взаємозв'язок між органами державної влади, бізнесом та громадянським суспільством;

– аналіз і синтез – застосовано для з'ясування змісту ключових понять («кіберстійкість», «інформаційний суверенітет», «гібридні загрози») та формування теоретичного базису дослідження;

– формально-юридичний метод – дозволив проаналізувати чинне законодавство України (Закони «Про національну безпеку», «Про основні засади забезпечення кібербезпеки»), виявити прогалини у регулюванні захисту критичної інфраструктури та окреслити шляхи імплементації європейської директиви NIS2;

– структурно-функціональний аналіз – використано для оцінки діяльності та розподілу повноважень між основними суб'єктами сектору безпеки (РНБО, Мінцифра, Міноборони, Держспецзв'язку), а також для аналізу ефективності роботи кластеру Brave1;

– порівняльний аналіз – покладено в основу вивчення міжнародного досвіду (США, Ізраїль, Естонія, Велика Британія) з метою адаптації кращих управлінських практик, таких як створення «Кіберліги» чи «цифрових посольств», до українських реалій;

– методи моделювання та прогнозування – застосовано у третьому розділі для розробки моделі Агенції оборонних інновацій та формулювання стратегічних рекомендацій щодо реформування державної політики у сфері оборонних технологій.

Практичне значення отриманих результатів полягає у розробці комплексу конкретних пропозицій та рекомендацій, спрямованих на підвищення ефективності системи публічного управління національною безпекою в умовах цифровізації та гібридної війни. Сформульовані в роботі положення доведені до рівня прикладних інструментів, що можуть бути використані органами державної влади у нормотворчій та організаційній діяльності.

Для вдосконалення законодавчої бази: Запропоновані зміни до нормативно-правових актів щодо врегулювання прав інтелектуальної власності у сфері оборонних технологій можуть бути використані профільними комітетами Верховної Ради України. Зокрема, йдеться про впровадження моделі, за якої майнові права залишаються за розробником, а держава отримує безвідкличну ліцензію на використання. Це дозволить стимулювати інновації та залучення венчурних інвестицій у сектор безпеки. Також обґрунтовано необхідність законодавчого закріплення статусу «цифрових посольств» для юридичного захисту державних реєстрів, розміщених у хмарних сховищах за кордоном.

Для оптимізації діяльності органів виконавчої влади: Рекомендації щодо трансформації кластеру Brave1 у повноцінну Агенцію оборонних досліджень та інновацій (за зразком ізраїльського директорату MAFAT) можуть бути імплементовані Кабінетом Міністрів України, Міністерством оборони та Міністерством цифрової трансформації. Запропонована структура агенції з

подвійним підпорядкуванням (військовим та уряду) дозволить скоротити шлях від розробки технології до її застосування на фронті.

Для реформування системи технічного захисту інформації: Обґрунтування переходу від статичної системи комплексної системи захисту інформації до ризик-орієнтованих підходів та декларування відповідності міжнародним стандартам (ISO/IEC 27001, NIST) може бути використане Адміністрацією Держспецзв'язку для дерегуляції ринку та пришвидшення впровадження ІТ-систем у секторі оборони.

Для вдосконалення кадрової політики: Розроблений механізм «технологічної мобілізації» та нові критерії бронювання ІТ-фахівців, що базуються на верифікованій кваліфікації та участі у критичних проєктах, а не лише на рівні заробітної плати, можуть бути використані Міністерством оборони та Міністерством економіки для збереження інтелектуального потенціалу держави.

Для освітньої сфери: Пропозиції щодо оновлення стандарту вищої освіти за спеціальністю 281 «Публічне управління та адміністрування» шляхом введення нових компетентностей («Управління цифровими проектами у публічному секторі», «Основи національної кіберстійкості») можуть бути використані Міністерством освіти і науки України та закладами вищої освіти при розробці освітньо-професійних програм підготовки магістрів.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1 Інформаційні технології як інструмент публічного управління у сфері національної безпеки в умовах гібридних загроз

В умовах глобальних геополітичних зрушень та стрімкої цифровізації суспільних відносин, система забезпечення національної безпеки зазнає фундаментальних трансформацій. Традиційні підходи до публічного управління у безпековій сфері, що базувалися на ієрархічних, жорстко регламентованих структурах та фізичному контролі території, втрачають свою ефективність перед лицем новітніх гібридних загроз. Сучасний етап державотворення в Україні, обтяжений повномасштабною збройною агресією, вимагає переосмислення теоретичних та практичних засад використання інформаційних технологій (ІТ) як ключового інструменту виживання та розвитку держави.

Актуальність даного дослідження обумовлена необхідністю формування нової парадигми публічного адміністрування, де ІТ виступають не допоміжним сервісом, а системоутворюючим фактором національної стійкості. Інформаційний простір перетворився на повноцінний театр воєнних дій, де об’єктами впливу стають критична інфраструктура, державні реєстри, процеси прийняття управлінських рішень та когнітивна сфера громадян. Це зумовлює потребу в глибокому аналізі наукових підходів до визначення місця та ролі ІТ в системі національної безпеки, дослідженні нормативно-правового регулювання цієї сфери та вивченні передового міжнародного досвіду.

У науці державного управління поняття «інформаційна безпека» пройшло

складний шлях еволюції, що відображає зміну технологічних укладів та характеру загроз. На початкових етапах, у рамках класичної теорії адміністрування, інформаційна безпека розглядалася переважно як технічна дисципліна, зосереджена на захисті каналів зв'язку та запобіганні витоку секретної інформації. Проте, сучасні виклики вимагають значно ширшого, міждисциплінарного підходу.

Сучасні українські вчені, зокрема О. Кононова, І. Кріцак, Я. Синяк, розглядають інформаційну безпеку як невід'ємну складову національної безпеки, що гарантує захищеність життєво важливих інтересів людини, суспільства і держави [47]. У цьому контексті інформаційні технології в публічному управлінні набувають подвійного значення: як об'єкт захисту (кібербезпека інфраструктури) та як інструмент забезпечення безпеки (системи моніторингу, аналітики, управління).

Парадигмальний зсув у теорії публічного управління полягає у переході від концепції «кібербезпеки» (cybersecurity) до концепції «кіберстійкості» (cyber resilience). Якщо традиційна безпека фокусується на побудові захисних периметрів для запобігання атакам, то стійкість, як категорія управління, передбачає здатність системи функціонувати в умовах перманентного деструктивного впливу, адаптуватися до змін у середовищі безпеки та швидко відновлювати свою функціональність після інцидентів [67].

Цей підхід корелює з теорією «New Public Governance», яка наголошує на мережевій взаємодії та залученні широкого кола стейкхолдерів до процесу управління. У сфері національної безпеки це означає, що держава більше не є монополістом у забезпеченні захисту; вона виступає координатором мережі, до якої входять приватні ІТ-компанії, оператори критичної інфраструктури, наукові установи та громадянське суспільство («білі хакери», волонтери).

Важливим аспектом теоретичного обґрунтування використання ІТ в системі національної безпеки є категорія «інформаційний суверенітет». У вітчизняному нормативному полі та науковій літературі цей термін часто визначається як виключне право держави формувати та реалізувати власну

інформаційну політику, розпоряджатися національними інформаційними ресурсами та захищати національний інформаційний простір від зовнішнього втручання [57].

Проте, серед науковців точаться гострі дискусії щодо доцільності та меж застосування цього поняття в епоху глобалізації. Критичний аналіз показує, що абсолютизація інформаційного суверенітету може вступати в конфлікт з принципами відкритого суспільства та вільного обміну інформацією. Експерти зазначають, що термін «інформаційний суверенітет» не є загальноприйнятим у міжнародному праві та може використовуватися для виправдання надмірного державного контролю або цензури [57].

Натомість, пропонується фокусуватися на «захисті національних інтересів в інформаційній сфері» та концепції «духовного суверенітету» або «когнітивної безпеки». Дослідники В. Карлова та Д. Мехеда акцентують увагу на тому, що загрози інформаційному суверенітету часто лежать не лише в технічній площині (кібератаки), але й у площині смислів та цінностей [47]. Гібридні загрози спрямовані на деформацію духовних цінностей суспільства, маніпуляцію суспільною думкою та підрив довіри до інститутів публічної влади. Відтак, завданням публічного управління стає не лише технічний захист інфраструктури, а й забезпечення ментальної стійкості нації через механізми стратегічних комунікацій та медіаграмотності.

Теоретичний базис функціонування системи публічного управління у сфері кібербезпеки спирається на низку принципів, які визначають вектор нормотворчої та правозастосовної діяльності. Аналіз наукових джерел [26] дозволяє виокремити ключові з них:

– Принцип пріоритетності запобіжних заходів (Precautionary Principle): Управління повинно бути проактивним, базуватися на аналізі ризиків та розвідці загроз (threat intelligence), а не лише на реагуванні на інциденти, що вже сталися.

– Принцип державно-приватного партнерства (Public-Private Partnership): Визнання того факту, що левова частка критичної інформаційної

інфраструктури перебуває у приватній власності, вимагає від органів публічної влади переходу від командно-адміністративних методів до партнерських моделей взаємодії.

– Принцип пропорційності та адекватності: Заходи із забезпечення безпеки не повинні створювати надмірних перешкод для розвитку цифрової економіки, інновацій та реалізації прав і свобод громадян. Регулювання має бути «мінімально необхідним» для досягнення цілей безпеки [59].

– Принцип стандартизації та інтероперабельності: Уніфікація національних стандартів кіберзахисту з міжнародними (ISO/IEC 27001, NIST, стандарти НАТО) є передумовою ефективної взаємодії з партнерами та інтеграції в євроатлантичні безпекові структури.

– Принцип об’єктивності та правової визначеності: Чітке законодавче визначення повноважень суб’єктів забезпечення кібербезпеки, категоризація об’єктів критичної інфраструктури та процедур реагування на інциденти.

Ці принципи формують теоретичну рамку, в якій розгортається практична діяльність органів публічної влади щодо використання ІТ в інтересах національної безпеки.

Сучасні гібридні загрози характеризуються безпрецедентною конвергенцією кінетичних, кібернетичних, економічних та інформаційно-психологічних впливів. В умовах цифрової доби, технології штучного інтелекту, Big Data та глобальна зв’язність перетворили інформаційний простір на домен ведення війни, що не поступається за значенням традиційним суші, морю чи повітрю.

Для системи публічного управління це означає необхідність протидії загрозам за кількома векторами одночасно:

– Фізичне та цифрове руйнування інфраструктури: Атаки на транспортні системи, енергетику та логістику часто поєднують фізичні удари з кібератаками на системи управління (SCADA), що вимагає скоординованої роботи служб надзвичайних ситуацій, кіберзахисту та військових [36].

– Інформаційні операції: Використання соціальних мереж та

ботоферм для поширення дезінформації, спрямованої на дестабілізацію суспільно-політичної ситуації, дискредитацію органів влади та зрив мобілізаційних заходів.

– Економічний кібершпіонаж: Викрадення інтелектуальної власності, комерційних таємниць та даних про стратегічні ресурси держави для підриву економічного потенціалу.

Динамічний характер цих загроз вимагає від системи публічного управління переходу до «цифрового врядування воєнного часу», де швидкість обробки інформації та прийняття рішень стає критичним фактором.

Яскравим прикладом практичної імплементації теоретичних засад мережецентричного управління є впровадження системи ситуаційної обізнаності «Delta». Ця національна військова система, розроблена Центром інновацій Міністерства оборони України, демонструє, як ІТ змінюють архітектуру управління безпекою [71].

Управлінські інновації системи Delta:

– Горизонтальна інтеграція: На відміну від традиційної вертикальної ієрархії, Delta забезпечує горизонтальний обмін даними між різними підрозділами та відомствами. Це руйнує відомчі «колодязі» (silos) та дозволяє формувати єдину картину оперативної обстановки в режимі реального часу.

– Data-Driven Decision Making: Публічне управління у сфері оборони переходить на рівень прийняття рішень на основі даних. Інтеграція інформації з супутників, дронів, радарів та чат-ботів дозволяє командуванню бачити поле бою комплексно, що підвищує точність та ефективність застосування ресурсів.

– Технологічна інтероперабельність з НАТО: Розробка системи за стандартами НАТО забезпечує технічну сумісність із системами партнерів, що є не лише військовим, а й політико-адміністративним досягненням, наближаючи інтеграцію України до Альянсу.

В умовах війни традиційні бюрократичні процедури державних закупівель та R&D виявляються занадто повільними. Відповіддю на цей виклик стало створення defense-tech кластеру Brave1 – платформи для розвитку

військових технологій [35].

Характеристика управлінської моделі Brave1:

– Міжвідомча координація: Засновниками кластеру виступили шість ключових державних органів: Мінцифра, Міноборони, Генштаб ЗСУ, РНБО, Мінстратегпром та Мінекономіки. Така структура дозволяє уникати дублювання функцій та забезпечує комплексний підхід до підтримки розробок – від ідеї до кодифікації та держконтракту.

– Сервісна модель держави: Замість директивного управління, держава виступає як провайдер сервісів (експертиза, доступ до полігонів, грантова підтримка, менторство) для приватних розробників та стартапів.

– Fast-track процедури: Кластер забезпечує пришвидшене проходження бюрократичних процедур допуску до експлуатації, скорочуючи шлях розробки від місяців до тижнів. Це є прикладом адаптивного публічного адміністрування, здатного змінювати власні регламенти заради результату.

Аналіз snippet-ів [52] свідчить про зростаючу роль технологій Big Data та штучного інтелекту (ШІ) в національній безпеці.

– Прогнозування та моделювання: Використання ШІ дозволяє аналізувати великі масиви даних для виявлення аномалій, прогнозування кібератак та моделювання сценаріїв кризових ситуацій.

– Автоматизація рутинних процесів: В публічному адмініструванні ШІ може взяти на себе функції моніторингу інформаційного простору, первинної обробки звернень громадян або аналізу логістичних ланцюгів, вивільняючи людський ресурс для стратегічних завдань.

– Етичні виклики: Впровадження ШІ у сферу безпеки породжує низку етичних та правових проблем (algorithmic bias, відповідальність за рішення ШІ), які потребують детального нормативного регулювання та громадського контролю для збереження демократичних цінностей [52].

Водночас, стрімка інтеграція новітніх технологій, зокрема штучного інтелекту, у контур національної безпеки актуалізує питання людського капіталу в системі публічного управління. Технології, якими б досконалими

вони не були, залишаються лише інструментом у руках управлінців. Тому цифрова трансформація безпекового сектору неминуче веде до зміни професійної моделі державного службовця. Сучасна теорія управління наголошує, що посадові особи, відповідальні за прийняття рішень у сфері безпеки, повинні володіти не лише правовими та адміністративними знаннями, а й високим рівнем цифрової грамотності. Розуміння принципів функціонування кіберпростору та навичок інформаційної гігієни стає такою ж базовою вимогою, як і знання державної мови. Без підготовленого персоналу навіть найсучасніші системи захисту можуть виявитися неефективними через банальні помилки користувачів або соціальну інженерію ворога.

Окремої уваги в теоретичному дискурсі заслуговує проблема технологічної залежності як загрози національній безпеці. В умовах гібридної війни використання програмного забезпечення або апаратного обладнання, виробленого країнами-агресорами чи ненадійними постачальниками, створює критичні вразливості для державної інфраструктури. Це зумовлює необхідність перегляду підходів до публічних закупівель та формування політики технологічного суверенітету. Публічне управління в цьому контексті має балансувати між потребою у швидкому доступі до інновацій та необхідністю ретельної перевірки походження технологій, що впроваджуються в органах влади та на об’єктах критичної інфраструктури.

Ще одним викликом для теоретичних засад публічного адміністрування є дисонанс між швидкістю розвитку технологій та інерційністю нормативно-правового регулювання. Класичні бюрократичні процедури, які передбачають тривалі етапи погоджень та експертиз, часто не встигають за динамікою кіберзагроз. Це вимагає від науковців та практиків пошуку нових, більш гнучких моделей нормотворчості. Мова йде про впровадження експериментальних правових режимів, які дозволяють сектору безпеки та оборони тестувати та використовувати новітні розробки без порушення загальних законодавчих рамок, забезпечуючи так звану «правову інтероперабельність» між потребами фронту та вимогами закону.

Тож, можна констатувати, що в умовах гібридних загроз інформаційні технології перестали виконувати виключно допоміжну, сервісну функцію. Вони трансформувалися у середовище існування самої системи національної безпеки. Ефективність публічного управління сьогодні вимірюється здатністю державних інституцій оперувати даними, захищати інформаційний периметр та забезпечувати безперервність управління державою навіть в умовах кризових ситуацій. Саме цей перехід від «ІТ як інструменту» до «ІТ як екосистеми» є ключовим теоретичним висновком, що визначає подальшу логіку дослідження механізмів забезпечення національної безпеки.

Розвиваючи думку про екосистемний підхід, варто заглибитися в аспект інформаційно-психологічного протиборства, який є невід'ємною частиною гібридних загроз. У цьому контексті інформаційні технології в системі публічного управління виконують роль не лише «щита» для захисту даних, а й активного інструменту формування смислів. Теоретичні моделі управління національною безпекою сьогодні все частіше оперують поняттям стратегічних комунікацій, реалізація яких неможлива без сучасних цифрових платформ. Держава повинна мати здатність не просто реагувати на дезінформацію чи фейки, а й випереджати їх, заповнюючи інформаційний простір достовірним контентом. Це вимагає від органів влади опанування алгоритмів роботи соціальних мереж та медіа-платформ, оскільки саме там формується суспільна думка та психологічна стійкість населення.

Окремого теоретичного осмислення потребує феномен «цифрового громадянського спротиву» або краудсорсингу у сфері безпеки, який став унікальною рисою українського досвіду. Традиційна теорія державного управління зазвичай розглядає громадянина як об'єкт захисту або отримувача адміністративних послуг. Натомість, сучасні реалії демонструють трансформацію громадянина у повноправного суб'єкта забезпечення національної безпеки. Завдяки мобільним застосункам та чат-ботам кожен власник смартфону перетворюється на сенсор системи ситуаційної обізнаності, передаючи дані про переміщення ворога чи наслідки обстрілів. Це створює

нову модель взаємодії «держава – суспільство», де інформаційні технології забезпечують безпрецедентну швидкість та масовість залучення населення до оборонних заходів, що було б неможливо реалізувати за допомогою класичних адміністративних механізмів.

Така децентралізація збору інформації, попри свою ефективність, породжує нові виклики для управлінської вертикалі, пов’язані з верифікацією даних. Величезний масив інформації, що надходить від відкритих джерел та громадян, вимагає впровадження в органах публічної влади автоматизованих систем аналізу та фільтрації. Без використання технологій обробки великих даних управлінська система ризикує бути перевантаженою інформаційним шумом, що може призвести до помилкових рішень або паралічу управління. Тому науковий дискурс зміщується від питання «як зібрати інформацію» до проблеми «як виокремити критично важливі знання з інформаційного потоку».

Крім внутрішнього виміру, використання інформаційних технологій суттєво змінює і зовнішньополітичний аспект забезпечення національної безпеки, формуючи явище цифрової дипломатії. Умовах гібридної війни здатність держави доносити свою позицію до міжнародної спільноти через цифрові канали стає фактором отримання військової та економічної допомоги.

Публічне управління у цій сфері виходить за межі традиційних дипломатичних протоколів, вимагаючи присутності державних інституцій на глобальних цифрових майданчиках, де відбувається боротьба за увагу світової аудиторії.

Це також актуалізує питання цифрового суверенітету, адже залежність комунікації від політики транснаціональних технологічних корпорацій, що володіють соціальними мережами, створює додаткові ризики для державної інформаційної політики.

1.2 Аналіз наукових підходів та нормативно-правового регулювання використання ІТ в інтересах національної безпеки

Правовий фундамент використання ІТ у безпековій сфері України формується на основі Конституції України, Закону України «Про національну безпеку України» та спеціального законодавства.

Закон України «Про основні засади забезпечення кібербезпеки України» є базовим актом, що визначає правові та організаційні основи захисту життєво важливих інтересів у кіберпросторі. Важливою новелою закону є закріплення принципів мінімально необхідного регулювання та державно-приватної взаємодії [59]. Закон легітимізує діяльність команд реагування на комп'ютерні надзвичайні події (CERT) та створює правові рамки для залучення волонтерських організацій до системи кіберзахисту [60].

Стратегія кібербезпеки України (2021-2025), розроблена з урахуванням методології Міжнародного союзу електрозв'язку (ITU), базується на реальній оцінці стану національної системи кібербезпеки. Цікавим є той факт, що при розробці стратегії проводилося опитування основних суб'єктів кібербезпеки, яке показало, що 83% респондентів представляли державний сектор [53]. Це свідчить про все ще домінуючу роль держави та необхідність більш активного залучення приватного бізнесу до формування політики.

Водночас, аналіз виявляє суттєві прогалини в законодавстві:

– Захист критичної інфраструктури: Законодавство у сфері захисту критичної інфраструктури (КІ) виявилося не повністю адаптованим до умов війни. Відсутність спеціального закону про захист критичної транспортної інфраструктури ускладнює координацію між відомствами та операторами транспорту в умовах гібридних атак [36].

– Відновлення інфраструктури: Існуючі нормативні акти не враховують специфіку швидкого відновлення зруйнованих об'єктів КІ за участю приватного капіталу, створюючи умови правової та фінансової

невизначеності для інвесторів [2].

Ключовим вектором розвитку нормативної бази є євроінтеграція, що передбачає гармонізацію українського законодавства з правом ЄС. Центральним елементом цього процесу є імплементація Директиви NIS2 (Network and Information Security Directive 2).

Основні положення NIS2 та їх вплив на Україну:

– Розширення сфери дії: Директива значно розширює перелік секторів, що підпадають під регулювання, включаючи енергетику, транспорт, охорону здоров'я, цифрову інфраструктуру, публічне управління, поштові послуги та управління відходами [39].

– Посилення відповідальності: NIS2 запроваджує пряму відповідальність вищого керівництва організацій (C-level management) за невиконання вимог кібербезпеки. Це змінює підхід до кібербезпеки з «проблеми ІТ-відділу» на «стратегічний ризик бізнесу/установи» [37].

– Безпека ланцюгів постачання: Директива вимагає від суб'єктів контролювати безпеку своїх постачальників. Для українських ІТ-компаній, що працюють з європейськими клієнтами, це означає необхідність повної відповідності стандартам ЄС для збереження доступу до ринку [42].

Виклики імплементації:

– Ресурсне забезпечення: Виконання вимог NIS2 потребує значних інвестицій у модернізацію систем захисту, впровадження багатофакторної аутентифікації, навчання персоналу та проведення регулярних аудитів. В умовах війни це створює додаткове навантаження на бюджет державних органів та підприємств [37].

– Кадровий потенціал: Дефіцит кваліфікованих фахівців з кібербезпеки, здатних впроваджувати нові стандарти, залишається критичною проблемою.

Держспецзв'язку активно працює над адаптацією українських стандартів до вимог NIS2 в рамках програми Ukraine Facility, розглядаючи це як необхідний крок для інтеграції України в Єдиний цифровий ринок ЄС [39].

Динамічний розвиток сфери цифровізації призвів до певної трансформації інституційного ландшафту та перерозподілу повноважень між органами влади. Показовим є кейс перерозподілу функцій між Міністерством цифрової трансформації (Мінцифра) та Державною службою спеціального зв'язку та захисту інформації (Держспецзв'язку).

З вересня 2023 року Мінцифра отримала статус центрального органу у сферах електронних комунікацій та радіочастотного ресурсу, перебравши ці функції від Держспецзв'язку [68]. Останнє зосередилося на своєму профільному завданні – захисті критичної інфраструктури, урядовому зв'язку та технічному захисті інформації. Такий крок спрямований на пришвидшення впровадження нових технологій (5G) та дерегуляцію телеком-ринку.

Однак, цей поділ вимагає високого рівня координації. Мінцифра, як драйвер цифровізації («держава у смартфоні»), прагне до максимальної швидкості та зручності сервісів, тоді як Держспецзв'язку відповідає за їх безпеку. Баланс між зручністю (usability) та безпекою (security) є класичною дилемою публічного управління, яка в Україні вирішується через механізми міжвідомчої взаємодії та роботу Національного координаційного центру кібербезпеки (НКЦК).

Інституційна модель забезпечення кібербезпеки в Україні побудована за принципом розподіленої відповідальності з координуючим центром. Основні суб'єкти та їхні функції представлені у Таблиці 1.

Таблиця 1.1 – Розподіл повноважень ключових суб'єктів національної системи кібербезпеки

Суб'єкт публічного управління	*Основні функції та сфера відповідальності*	*Нормативна основа*
РНБО (НКЦК)	Стратегічна координація всіх суб'єктів сектору безпеки і оборони, затвердження стратегій, управління кризовими ситуаціями національного рівня.	ЗУ «Про нацбезпеку», Укази Президента [53].
Міністерство цифрової трансформації	Формування державної політики у сфері цифровізації, розвиток ІТ-інфраструктури, електронні довірчі послуги, ШІ, віртуальні активи, адміністрування «Дії» та Brave1.	Положення про Міністерство [55].

Продовження таблиці 1.1

Суб'єкт публічного управління	*Основні функції та сфера відповідальності*	*Нормативна основа*
Держспецзв'язку (SSSCIP)	Захист державних інформаційних ресурсів, кіберзахист об'єктів критичної інфраструктури, урядовий зв'язок, криптографічний захист, імплементація NIS2, CERT-UA.	ЗУ «Про Держспецзв'язку» [68].
Служба безпеки України (СБУ)	Боротьба з кібертероризмом, кібершпигунством, контррозвідувальний захист інтересів держави у кіберпросторі, розслідування злочинів проти основ нацбезпеки.	ЗУ «Про СБУ»
Кіберполіція (НПУ)	Протидія загальнокримінальній кіберзлочинності (шахрайство, піратство), захист прав громадян у мережі, превентивна робота.	ЗУ «Про Національну поліцію»
Міністерство оборони / ЗСУ	Кібероборотьба у воєнній сфері, захист військових систем управління (C4ISR), розвиток ситуаційної обізнаності (Delta).	Воєнна доктрина [71].
Національний банк України	Забезпечення кіберстійкості банківської системи та системи електронних платежів.	ЗУ «Про НБУ»

Мінцифра займає унікальне місце в системі, виступаючи «архітектором» цифрової держави. Її повноваження виходять за рамки простого впровадження ІТ; вони включають формування політики у сферах штучного інтелекту, блокчейну, віртуальних активів та розвитку цифрової грамотності населення [55].

Функція Мінцифри полягає не лише в наданні послуг, а й у створенні екосистеми, де технології стають драйвером економічного зростання та безпеки. Проте, масштабна цифровізація (централізація даних у реєстрах, портал «Дія») створює нові ризики. Концентрація даних в одній точці доступу робить систему привабливою мішенню для ворога, що вимагає безпрецедентних заходів безпеки та постійної взаємодії з Держспецзв'язку та СБУ.

Інституційна спроможність України значно посилюється завдяки тісній співпраці з міжнародними партнерами.

– USAID: Проєкт «Кібербезпека критично важливої інфраструктури України» надає технічну допомогу, проводить навчання фахівців та допомагає у розробці законодавства [25].

– e-Governance Academy (Естонія): Спільно з Держспецзв'язку реалізує проєкти з підвищення кіберстійкості, навчання державних службовців та обміну досвідом побудови захищених систем.

– Tallinn Mechanism: Формат координації допомоги у сфері кібербезпеки, що об'єднує зусилля країн-донорів для задоволення нагальних потреб України у кіберзахисті.

Ця допомога не обмежується фінансами; вона включає трансфер знань, методологій та інтеграцію українських фахівців у глобальну професійну спільноту.

Для вдосконалення національної системи доцільно проаналізувати моделі управління провідних країн, які демонструють високу ефективність у протидії кіберзагрозам.

Естонська модель є еталоном для малих цифрових держав. Вона базується на концепції, що кібербезпека є спільною справою всього суспільства.

– Кіберліга (Cyber Defense Unit): Унікальне добровольче формування у складі воєнізованої організації Kaitseliit. Воно об'єднує провідних IT-фахівців приватного сектору, які у вільний від роботи час беруть участь у навчаннях та забезпечують захист держави у кризових ситуаціях. Це дозволяє державі мати доступ до висококласної експертизи без необхідності конкурувати зарплатами з бізнесом.

– Публічно-приватне партнерство: Естонія однією з перших ухвалила законодавство (прообраз NIS Directive), яке зобов'язало банки та телекоми співпрацювати з державою у питаннях безпеки.

– Освіта: Обов'язкові курси кібергігієни для держслужбовців та широкі просвітницькі кампанії для населення є фундаментом національної стійкості [3].

Британська модель характеризується створенням потужного централізованого органу – National Cyber Security Centre (NCSC).

– Інституційна прозорість: NCSC є частиною розвідувальної служби

GCHQ, але працює публічно, надаючи рекомендації та підтримку як уряду, так і бізнесу та громадянам [10].

– Cyber Governance Code of Practice: Уряд Британії активно просуває стандарти корпоративного управління, які покладають відповідальність за кіберризики безпосередньо на ради директорів компаній. Кібербезпека розглядається на рівні з фінансовими ризиками [5].

– Active Cyber Defence: Стратегія передбачає проактивні заходи з нейтралізації загроз ще до того, як вони досягнуть користувачів (наприклад, блокування фішингових сайтів на рівні провайдерів).

Модель США, реалізована через Агентство з кібербезпеки та безпеки інфраструктури (CISA), фокусується на захисті критичної інфраструктури та оперативній співпраці.

– JCDC (Joint Cyber Defense Collaborative): Унікальна платформа, де урядові аналітики та представники технологічних гігантів (Amazon, Google, CrowdStrike, Microsoft) спільно планують операції та обмінюються даними про загрози в реальному часі [17].

– Секторальний підхід: CISA координує захист 16 секторів критичної інфраструктури, тісно взаємодіючи з профільними міністерствами (Sector Risk Management Agencies) [8].

– Міжнародна підтримка: CISA має прямий меморандум про співпрацю з українським Держспецзв'язку, що дозволяє оперативно обмінюватися даними про російські кіберзагрози, які часто є спільними для обох країн [6].

Національний кібердиректорат Ізраїлю (INCD) реалізує модель, де безпека є драйвером економічного розвитку.

– Cyber Net: Захищена соціальна мережа для фахівців з кібербезпеки, що дозволяє тисячам організацій обмінюватися інформацією про атаки та вразливості в режимі реального часу [31].

– Стимулювання R&D: INCD активно підтримує стартапи та наукові дослідження, перетворюючи кіберзагрози на можливості для експорту

технологій [12].

– Методологія: Ізраїль адаптував американський стандарт NIST Cybersecurity Framework, створивши на його основі зрозумілу та практичну методологію захисту для організацій будь-якого розміру [11].

Таблиця 1.2 – Порівняльна характеристика моделей управління кібербезпекою

Характеристика	*Україна*	*Естонія*	*Велика Британія*	*США*	*Ізраїль*
Ключовий орган	НКЦК (координація), Держспецзв'язку, Мінцифра	RIA (Information System Authority)	NCSC (частина GCHQ)	CISA (частина DHS)	INCD (підпорядкований Прем'єр-міністру)
Модель взаємодії з бізнесом	Змішана, розвивається через NIS2	Інтегрована, обов'язкова для КІ	Консультативна, стандартизація	Операційна співпраця (JCDC)	Екосистемна, R&D орієнтована
Залучення громадян	IT Army (неформальне), волонтери	Кіберліга (формалізоване волонтерство)	Cyber First (освіта)	Awareness campaigns	Cyber education programs
Підхід до стандартів	Гармонізація з ЄС (NIS2), ISO	Основа для стандартів ЄС	Cyber Assessment Framework	NIST Framework	Адаптований NIST (ICDM)

Українська наукова спільнота, зокрема школи Інституту інформації, безпеки і права НАПрН України, активно працює над теоретичним осмисленням нових реалій. Дослідження фокусуються на проблемах правового забезпечення оборони, кібернетичної безпеки та правової інформатики [32].

Науковці наголошують на необхідності подальшого вивчення впливу квантових технологій на криптографічний захист, етичних аспектів використання ШІ в системах безпеки та психологічних наслідків гібридних операцій [52]. Також актуальним є дослідження балансу між прозорістю влади та необхідністю обмеження інформації в умовах війни.

– Кадровий дефіцит та розвиток людського капіталу: Конкуренція з приватним сектором за IT-фахівців залишається гострою проблемою. Державна служба часто не може запропонувати ринкові зарплати. Вирішенням може

стати масштабування естонського досвіду «Кіберліги» або запровадження спеціальних форм проходження служби для ІТ-фахівців (кібервійська).

– Технологічна залежність vs Цифровий суверенітет: Україна успішно використала хмарні технології світових гігантів (Amazon, Microsoft) для порятунку державних реєстрів. Однак, у довгостроковій перспективі це породжує питання залежності від зовнішніх провайдерів та необхідності формування політики «цифрового суверенітету».

– Фінансування відновлення: Відновлення зруйнованої критичної інфраструктури потребує колосальних коштів (понад $5 млрд лише на термінове відновлення за даними звітів). Відсутність чітких механізмів страхування воєнних ризиків та державно-приватного партнерства гальмує залучення інвестицій [2].

– Інтеграція воєнного та цивільного секторів: Війна показала ефективність подвійного використання технологій (dual-use). Система публічного управління має бути достатньо гнучкою, щоб інтегрувати цивільні інновації у військовий сектор (приклад Brave1) та навпаки.

На основі проведеного аналізу пропонуються наступні кроки:

– Завершення імплементації NIS2: Прискорення прийняття підзаконних актів, що деталізують вимоги директиви, та проведення масштабної роз’яснювальної роботи з бізнесом.

– Формалізація волонтерського руху: Створення законодавчої бази для діяльності «білих хакерів» та кіберволонтерів, надання їм правового статусу та соціальних гарантій.

– Розвиток інституційної спроможності: Посилення аналітичних підрозділів НКЦК та Держспецзв’язку, впровадження сучасних систем threat intelligence та автоматизованого обміну даними про інциденти.

– Удосконалення законодавства про КІ: Прийняття спеціалізованих законів щодо захисту окремих секторів (транспорт, енергетика) з урахуванням уроків війни.

Проведене глибоке дослідження теоретичних та практичних засад

використання інформаційних технологій в системі забезпечення національної безпеки дозволяє сформулювати наступні узагальнення:

По-перше, відбулася фундаментальна зміна об'єкта та суб'єкта управління. Інформаційні технології трансформувалися з інструментарію забезпечення діяльності органів влади в самостійний простір реалізації державної політики та національних інтересів. Кіберпростір офіційно визнано доменом ведення бойових дій, що вимагає відповідної адаптації теорії та практики публічного адміністрування.

По-друге, зміна парадигми безпеки. Традиційна концепція «абсолютного захисту» поступилася місцем концепції «кіберстійкості» (cyber resilience). Це вимагає від органів публічної влади впровадження ризик-орієнтованого підходу, де здатність до відновлення та адаптації є не менш важливою, ніж здатність відбивати атаки.

По-третє, інституційна адаптивність. Українська модель управління безпекою в умовах війни продемонструвала високу здатність до адаптації та інновацій. Створення кластеру Brave1, впровадження системи Delta та цифровізація державних послуг через «Дію» є прикладами ефективного «гнучкого управління» (agile governance). Водночас, існують виклики у сфері координації повноважень та нормативного регулювання захисту критичної інфраструктури.

По-четверте, міжнародна інтеграція. Майбутнє національної системи безпеки нерозривно пов'язане з інтеграцією в євроатлантичні структури. Гармонізація законодавства з вимогами ЄС (NIS2) та стандартами НАТО є не лише політичним зобов'язанням, а й технологічною необхідністю для забезпечення сумісності систем та ефективної колективної безпеки.

Теоретичні засади, що формуються сьогодні в Україні під впливом гібридної війни, мають унікальний характер. Емпіричний досвід протидії повномасштабній кіберагресії, осмислений науковою спільнотою та закріплений у нормативних актах, стає внеском України у розвиток глобальної теорії публічного управління безпекою.

Розвиваючи тезу про унікальність українського досвіду, варто акцентувати увагу на тому, що вітчизняна наука державного управління нині вирішує надскладне завдання: як інтегрувати жорсткі, часом авторитарні методи воєнного часу в демократичну канву європейського законодавства. Наукові дискусії все частіше точаться навколо поняття «алгоритмічного врядування» та ризиків, які воно несе для прав людини. Дослідники наголошують, що нормативно-правове регулювання використання ІТ у безпековій сфері не повинно обмежуватися лише технічними регламентами захисту інформації. Воно має включати чіткі етичні протоколи використання великих даних та штучного інтелекту, аби запобігти перетворенню інструментів безпеки на інструменти тотального цифрового контролю над громадянами.

Саме тому в науковому середовищі кристалізується думка про необхідність переходу від статичного законодавства до більш гнучких форм правового регулювання, так званого «soft law» або м’якого права. В умовах, коли технології змінюються швидше, ніж Верховна Рада ухвалює закони, науковці пропонують розширити повноваження виконавчих органів, зокрема НКЦК та Держспецзв’язку, щодо встановлення динамічних стандартів кібербезпеки. Такий підхід дозволить миттєво адаптувати нормативну базу під нові вектори атак, не проходячи довгі бюрократичні процедури, що є критично важливим для збереження керованості державою в умовах гібридної війни.

Таким чином, аналіз наукових джерел та нормативно-правової бази засвідчує, що в Україні відбувається формування нової екосистеми публічного управління безпекою. Вона характеризується відходом від суто відомчого підходу на користь мережецентричної моделі, де правові норми слугують не бар’єром, а каркасом для взаємодії державних органів, бізнесу та громадянського суспільства. Це створює надійне підґрунтя для подальшого практичного дослідження ефективності цих механізмів, до якого ми перейдемо в наступних розділах роботи.

РОЗДІЛ 2
АНАЛІЗ ПРАКТИКИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ СУБ'ЄКТАМИ ПУБЛІЧНОГО УПРАВЛІННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

2.1 Оцінка поточного стану впровадження та використання ІТ в діяльності органів сектору безпеки і оборони України

Сучасна архітектура національної безпеки України формується в умовах безпрецедентних викликів, пов'язаних із повномасштабною збройною агресією Російської Федерації. У цьому контексті інформаційні технології (ІТ) трансформувалися з допоміжного інструменту адміністрування у критично важливий домен ведення війни та забезпечення життєдіяльності держави. Публічне управління у сфері безпеки і оборони зазнало фундаментальних змін, переходячи від ієрархічних, паперових моделей до мережецентричних, цифрових екосистем.

Цифрова трансформація сектору безпеки і оборони України відбувається в умовах «Першої світової кібервійни», що вимагає від суб'єктів публічного управління не лише модернізації технічної бази, але й докорінного перегляду управлінських процесів, нормативного регулювання та кадрової політики.

Система публічного управління у сфері кібербезпеки та оборонних ІТ характеризується розподіленою відповідальністю, де кожен суб'єкт виконує специфічні функції, що часто перетинаються, створюючи як синергію, так і управлінські колізії.

РНБО виступає ключовим стратегічним координатором, що визначає пріоритети державної політики у сфері кібербезпеки. Після 2022 року роль РНБО трансформувалася від дорадчого органу до оперативного центру прийняття рішень через Національний координаційний центр кібербезпеки (НКЦК).

Діяльність НКЦК зосереджена на консолідації зусиль усіх суб'єктів сектору безпеки. Важливим кроком у 2024 році стало ініціювання створення першого національного кіберполігону «Cyber Range UA» [23]. Цей проєкт демонструє перехід від теоретичної підготовки фахівців до практичного відпрацювання сценаріїв реагування на кіберінциденти в умовах, наближених до бойових. Публічне управління в цьому аспекті набуває ознак сервісної моделі, де держава надає інфраструктуру для підвищення кваліфікації як державних, так і приватних фахівців.

Стратегічні комунікації РНБО також зазнали змін. Публікація регулярних звітів, таких як «Cyber Digest», свідчить про впровадження культури прозорості та обізнаності (situational awareness) на національному рівні [23]. РНБО фіксує тенденції кібервійни, наголошуючи на гібридному характері загроз, де кібератаки на енергетичну та фінансову інфраструктуру супроводжуються інформаційно-психологічними операціями. Аналіз діяльності РНБО показує, що орган намагається інтегрувати міжнародну допомогу (зокрема, USAID) для побудови стійкої архітектури кіберзахисту, однак питання ефективності координації між різними відомствами залишається відкритим.

Мінцифри є унікальним феноменом у системі публічного управління України, оскільки, будучи цивільним міністерством, воно фактично взяло на себе лідерство у впровадженні оборонних інновацій. Це створює нову модель «цивільно-військового злиття» (civil-military fusion), характерну для держав, що перебувають у стані тотальної війни.

Стратегія розвитку електронних комунікацій до 2030 року, презентована Мінцифри, чітко визначає інтернет та зв'язок як домени ведення війни [49]. Міністерство не обмежується цифровізацією адміністративних послуг, а активно втручається в процеси оборонних закупівель та розробки озброєнь. Співпраця з Національним антикорупційним бюро (НАБУ) для моніторингу закупівель безпілотних літальних апаратів (БПЛА) демонструє застосування ІТ як інструменту антикорупційного комплаєнсу в секторі оборони [38]. Це дозволяє мінімізувати корупційні ризики, які традиційно є високими у закритих

оборонних бюджетах.

Ключовим досягненням Мінцифри є створення кластера оборонних технологій Brave1, який діє як єдине вікно для інноваторів, держави та військових. Ця платформа замінює традиційні бюрократичні процедури прийняття озброєння на експлуатацію (які могли тривати роками) на прискорені треки (fast-track), що є революційним для української системи публічного адміністрування [16].

Міністерство оборони України проходить складний шлях цифрової трансформації, спрямований на відмову від «паперової армії» та впровадження принципів прозорості та підзвітності.

Важливим елементом цієї трансформації є діяльність Державного оператора тилу (ДОТ), який у 2024 році успішно пройшов незалежний фінансовий аудит компанією AC Crowe Ukraine. Аудит підтвердив ефективність використання цифрових рішень, таких як «DOT-Chain» та «DOT-xRM», які дозволяють повністю оцифрувати процес постачання – від заявки до акту прийому-передачі [40]. Обробка понад 59 000 актів в електронному форматі лише за один рік свідчить про масштабність змін. Рекомендації аудиторів щодо консолідації документації в електронному форматі вказують на те, що повна відмова від паперу ще не відбулася, але вектор руху обрано вірно.

Збройні Сили України виступають безпосередніми користувачами та замовниками бойових інформаційних систем. Впровадження системи ситуаційної обізнаності DELTA, розробленої Центром інновацій Міноборони, стало проривом у військовій справі. Система дозволяє інтегрувати дані з різних джерел розвідки (HUMINT, SIGINT, IMINT) та забезпечувати обмін даними в режимі реального часу [70]. Проте, використання таких систем вимагає високого рівня цифрової грамотності особового складу та надійної інфраструктури зв’язку, що не завжди доступна на «нулі».

Держспецзв’язку виконує подвійну функцію: регулятора у сфері криптографічного та технічного захисту інформації та оператора кіберзахисту державних ресурсів.

Діяльність служби у 2024 році стала об’єктом пильної уваги контролюючих органів. Звіт Рахункової палати виявив порушення та недоліки на суму понад 5,2 млрд грн, зокрема під час закупівель безпілотних систем [41]. Це свідчить про системну проблему: застаріла нормативно-правова база не встигає за швидкістю закупівель, необхідних в умовах війни. Недосконалість регламентних документів створює ситуацію, коли оперативні рішення, життєво необхідні для фронту, можуть кваліфікуватися як фінансові порушення.

Водночас, підрозділ CERT-UA, що діє при Держспецзв’язку, демонструє високу ефективність у виявленні та нейтралізації кіберзагроз. Аналіз звітів CERT-UA показує зміщення фокусу атак ворога з деструктивних дій (wiperware) на кібершпигунство та тривалу присутність у системах [72].

СБУ фокусується на контррозвідувальному захисті інтересів держави у кіберпросторі та розслідуванні кіберзлочинів. Взаємодія СБУ з іншими суб’єктами, зокрема через обмін індикаторами компрометації (IoC), є критичною для національної безпеки. Спецслужба також протидіє інформаційно-психологічним операціям ворога, блокуючи ботоферми та виявляючи агентів впливу в цифровому середовищі. Звіти вказують на активне використання ворогом методів соціальної інженерії, де зловмисники маскуються під представників СБУ для розповсюдження шкідливого програмного забезпечення [72], що вимагає від СБУ постійного вдосконалення методів верифікації та комунікації з громадськістю.

Технологічний ландшафт сектору безпеки і оборони України представляє собою строкату суміш державних розробок, волонтерських ініціатив та успадкованих систем. Головним викликом є забезпечення їх інтероперабельності (взаємосумісності).

Системи управління боєм є «нервовою системою» сучасної армії. В Україні склалася унікальна ситуація співіснування двох потужних екосистем.

Система «DELTA» – це хмарна платформа, побудована за стандартами НАТО. Вона забезпечує об’єднану картину поля бою (Common Operational Picture). Функціонал DELTA дозволяє планувати операції, наносити обстановку

та обмінюватися даними про ворога в захищеному контурі. Система є кросплатформною та веб-орієнтованою, що дозволяє використовувати її на будь-якому пристрої [70]. Важливою перевагою є можливість інтеграції потоків з дронів. Міністерство оборони активно працює над інтеграцією різних типів БПЛА до DELTA для «розумного планування» [70].

Програмний комплекс «Кропива» – розробка волонтерської організації «Армія SOS», яка фокусується на тактичній ланці, зокрема на управлінні артилерійським вогнем. Вона працює на Android-пристроях і дозволяє автоматизувати розрахунки стрільби, що значно скорочує час від виявлення цілі до її ураження [44].

Таблиця 2.1 – Порівняльний аналіз та проблеми інтеграції:

Характеристика	*DELTA*	*Кропива*
Походження	Державна (Центр інновацій МОУ)	Волонтерська (Армія SOS)
Рівень управління	Оперативно-тактичний, Стратегічний	Тактичний (батарея, дивізіон)
Архітектура	Хмарна (Cloud-native)	Автономна (Офлайн карти + P2P)
Стандарти	Сумісність з НАТО (JADC2)	Власні протоколи
Користувачі	Штаби, ситуаційні центри	Артилеристи, розвідка на місцях

Основною проблемою залишається відсутність повної автоматизованої взаємодії між цими системами. Хоча обидві системи впроваджуються в навчальний процес (наприклад, в Національній академії НГУ), на практиці військові часто змушені вручну переносити координати з однієї системи в іншу. Артилеристи віддають перевагу «Кропиві» за її автономність та швидкість розрахунків, тоді як штаби використовують DELTA для загального бачення [44]. Ця фрагментація (data silos) знижує ефективність «Kill Web» – концепції миттєвого ураження, яку намагається впровадити Міноборони [48].

Система «Оберіг» (Єдиний державний реєстр призовників, військовозобов’язаних та резервістів) стала наріжним каменем цифрової мобілізації. У 2024 році функціонал реєстру було значно розширено за рахунок інтеграції з іншими державними базами даних: Податковою службою, РАЦС, Міграційною службою, МОН та Прикордонною службою [1].

Проблеми функціонування:

– Якість даних: Верифікація даних відбувається автоматично, але історичні помилки в паперових справах призводять до некоректних статусів у реєстрі. Громадяни часто не знаходять себе в реєстрі або бачать застарілу інформацію, що змушує їх фізично відвідувати ТЦК, нівелюючи ідею цифровізації [69].

– Захист персональних даних: Правозахисники висловлюють занепокоєння щодо концентрації надмірної кількості чутливої інформації в одній базі даних. Хоча законодавство про захист персональних даних передбачає винятки в інтересах національної безпеки, відсутність прозорого логування доступу («історії змін») для самого користувача створює ризики зловживань та корупції [1].

– Кібербезпека: Централізовані реєстри є пріоритетною ціллю для ворожих хакерів. Захист «Оберегу» вимагає не лише технічних засобів, але й суворих процедур допуску операторів (співробітників ТЦК), що на практиці складно забезпечити в умовах плинності кадрів.

Впровадження SAP (Systemanalyse Programmentwicklung) у Міноборони для управління ресурсами є спробою привести українську військову логістику до стандартів НАТО. Системи класу ERP (Enterprise Resource Planning) дозволяють бачити залишки на складах у реальному часі. Однак, перехід від радянської системи обліку до SAP наштовхується на «культурний опір» на місцях та необхідність перенавчання тисяч логістів. Аудит DOT підтвердив, що перехід на цифрові акти (DOT-Chain) значно пришвидшив процеси, але також висвітлив необхідність повної відмови від паперового дублювання, яке все ще вимагається деякими нормативними актами [40].

Попри значний прогрес, впровадження IT у секторі безпеки стикається з низкою критичних проблем.

Український оборонний сектор перебуває під постійним тиском кібератак. Групи, асоційовані з російськими спецслужбами (наприклад, UAC-0185, UAC-0050, Turla), змінили тактику. Замість масових DDoS-атак

вони фокусуються на цільовому фішингу (spear phishing) через месенджери Signal та WhatsApp, намагаючись викрасти облікові дані до систем DELTA та Кропива [14].

Звіти CERT-UA за 2024 рік фіксують випадки компрометації VPN-акаунтів, які залишалися непоміченими протягом року [72]. Це свідчить про недостатній рівень моніторингу мережевої активності та контролю доступу підрядників. Використання соціальної інженерії (повідомлення про «полонених», «нагороди») експлуатує емоційний стан військових та їхніх родин.

Однією з найгостріших проблем є забезпечення IT-сектору кваліфікованими кадрами. Поточна система бронювання (reservation) виявилася неефективною для IT-галузі. Станом на 2024 рік було заброньовано лише близько 11 тисяч IT-фахівців, що є мізерною кількістю порівняно з енергетичним (163 тис.) чи аграрним секторами [51].

Основна причина – невідповідність критеріїв бронювання (офіційне працевлаштування, середня зарплата по регіону) реаліям IT-ринку, де 80% фахівців працюють як ФОП (гіг-контрактори). Це створює парадоксальну ситуацію: держава потребує висококласних кіберфахівців для захисту критичної інфраструктури та розробки MilitaryTech, але механізми мобілізації часто відправляють цих людей в піхоту, де їхні унікальні навички не використовуються ефективно. Відсутність гнучкого механізму «технологічної мобілізації» загрожує втратою інтелектуального потенціалу нації.

Використання хмарних технологій (Cloud Computing) для зберігання оборонних даних тривалий час було заблоковане застарілим законодавством, яке вимагало фізичного розміщення серверів на території України (data sovereignty). Хоча після 2022 року були внесені зміни, що дозволяють використовувати хмари країн НАТО, проблема юридичної визначеності залишається.

Зокрема, концепція «цифрової держави» в екзилі потребує чіткого механізму «даних посольств» (Data Embassies), де дані користуються

дипломатичним імунітетом. Українське законодавство поки що фрагментарно регулює ці питання, що створює ризики для довгострокового зберігання критичних реєстрів за кордоном [15]. Крім того, процедури закупівлі хмарних послуг державними органами залишаються складними та забюрократизованими.

Логічним продовженням інфраструктурних викликів є питання забезпечення стійкого зв'язку, який виступає фундаментом для всіх згаданих цифрових екосистем. Унікальність української ситуації полягає в тому, що критична комунікаційна архітектура держави значною мірою залежить від приватної іноземної компанії. Масове використання терміналів супутникового зв'язку Starlink створило прецедент, коли стратегічна спроможність системи управління військами залежить від корпоративних рішень та політичної волі третьої сторони. Для теорії публічного управління це формує новий парадокс: держава делегує частину свого суверенітету у сфері зв'язку приватному провайдеру заради забезпечення життєздатності системи оборони. Це вимагає від органів влади не лише технічної експертизи, а й постійної «технологічної дипломатії» для гарантування безперебійності сервісу.

Окрім того, оцінюючи поточний стан, неможливо оминути проблему інтеграції західних зразків озброєння в єдиний інформаційний контур. Оскільки Україна отримує допомогу від десятків країн-партнерів, сектор безпеки стикається з так званим «зоопарком технологій». Кожна сучасна артилерійська система чи засіб ППО має власне програмне забезпечення, яке часто не сумісне з українськими системами ситуаційної обізнаності. Управлінський виклик тут полягає в необхідності створення програмних «містків» та шлюзів, які б дозволили об'єднати різнорідні дані в єдину картину. Це завдання лягає на плечі як штатних військових програмістів, так і волонтерських спільнот, що знову підкреслює гібридний, державно-громадський характер управління в цій сфері.

Варто також звернути увагу на розрив між високим рівнем розробки програмного забезпечення центрального рівня та реаліями його експлуатації «в

полях». Попри наявність передових систем типу DELTA, значна частина документообігу на тактичному рівні все ще ведеться в паперовому вигляді або через незахищені побутові месенджери. Людський фактор залишається слабкою ланкою: в умовах фізичного виснаження та стресу військовослужбовці схильні нехтувати складними протоколами кібербезпеки заради швидкості передачі інформації. Це свідчить про те, що впровадження ІТ в секторі оборони – це не лише написання коду, а й масштабна просвітницька та адміністративна робота зі зміни організаційної культури, яка на даному етапі ще далека від завершення.

Таким чином, поточний стан використання ІТ в секторі безпеки і оборони можна охарактеризувати як стан «адаптивного хаосу», що поступово структурується. Система демонструє феноменальну стійкість та інноваційність знизу, проте все ще потребує жорсткішої стандартизації, легалізації волонтерських рішень та вирішення фундаментальних питань кадрового забезпечення зверху.

Окремий пласт проблем у системі публічного управління безпекою становить феномен так званої «тіньової цифровізації». Значна частина технічних засобів, які забезпечують роботу системи ситуаційної обізнаності на тактичному рівні – ноутбуки, планшети, роутери, камери відеоспостереження – потрапляють до підрозділів через волонтерські канали і часто не ставляться на офіційний баланс військових частин. З точки зору бюрократичної логіки мирного часу, це створює управлінську колізію: держава де-факто управляє військами через обладнання, яке де-юре їй не належить і яке вона не може офіційно обслуговувати чи списувати. Це змушує командирів вести подвійну бухгалтерію та шукати неформальні шляхи ремонту критично важливої техніки, що відволікає управлінський ресурс від виконання бойових завдань.

Разом з тим, варто відзначити інституційну еволюцію у сфері використання розвідувальної інформації. Якщо раніше монополія на збір та аналіз даних належала виключно державним спецслужбам, то сьогодні ми спостерігаємо ефективну інтеграцію OSINT-спільнот (розвідка на основі

відкритих джерел) у державний контур прийняття рішень. Діяльність таких проєктів, як DeepState чи Molfar, продемонструвала, що громадські організації здатні верифікувати дані та формувати аналітичні продукти швидше за громіздкі державні структури. Публічне управління в цьому аспекті демонструє гнучкість, легалізуючи використання таких даних при плануванні операцій та інформуванні суспільства, що раніше вважалося б порушенням протоколів секретності.

Ще одним важливим вектором змін є створення Сил безпілотних систем як окремого роду військ. Це рішення є не просто військовим, а насамперед управлінським прецедентом, який закріплює технологічну домінантну в структурі Збройних Сил. З точки зору публічного адміністрування, це спроба масштабувати успішні низові практики застосування роботизованих систем до рівня державної політики.

Це вимагає від системи управління повної перебудови логістичних ланцюжків, адже забезпечення дронами та комплектуючими за своєю динамікою більше нагадує роботу IT-дистриб'ютора, ніж класичне військове постачання.

Окрім суто військового виміру, використання IT органами сектору безпеки все більше проникає у сферу прогнозування соціально-економічних ризиків. Рада національної безпеки і оборони через модуль «СОТА» намагається моніторити не лише перебіг бойових дій, а й стан продовольчої безпеки, енергетики та демографії. Проте на практиці інтеграція даних від різних міністерств часто гальмується через відомчу розрізненість та відсутність єдиних стандартів метаданих. Кожне відомство продовжує накопичувати дані у власних форматах, що ускладнює їх автоматизоване зведення в єдину аналітичну панель для вищого військово-політичного керівництва держави.

2.2 Міжнародний досвід публічного управління у сфері впровадження ІТ для протидії загрозам національній безпеці

Для подолання виявлених проблем Україні необхідно звернутися до досвіду держав, які побудували ефективні моделі цифрової оборони. Аналіз досвіду США, Ізраїлю, Естонії та НАТО дозволяє виділити ключові патерни успіху та уникнути помилок.

Модель США базується на чіткому розмежуванні повноважень, потужній інституційній спроможності та глибокій інтеграції з приватним сектором.

CISA (Cybersecurity and Infrastructure Security Agency) є центральним органом, відповідальним за захист критичної інфраструктури. Її структура включає Об'єднаний центр кіберзахисту (JCDC), який об'єднує урядові агенції, індустріальних гігантів та міжнародних партнерів для оперативного обміну інформацією про загрози.

Урок для України: Україна намагається відтворити цю модель через НКЦК, але американський досвід показує, що ключ до успіху лежить не в адміністративному підпорядкуванні, а в довірі приватного сектору. CISA позиціонує себе як партнер, а не каральний орган, надаючи бізнесу інструменти для самозахисту (Shields Up).

Негативний досвід (Administrative Warning): Важливим уроком є невдача CISA у реалізації програми утримання персоналу (Cyber Incentive Program). Звіт Генерального інспектора DHS виявив, що понад 100 млн доларів було витрачено неефективно, а бонуси отримували працівники, чиї функції не були критичними для кібербезпеки [9]. Це застереження для Міноборони України при розробці системи мотивації для майбутніх Кіберсил: фінансові стимули повинні бути чітко прив'язані до кваліфікації та ролі фахівця, а не просто до факту служби в ІТ-підрозділі.

DIU (Defense Innovation Unit) – це організація Пентагону, створена для прискорення впровадження комерційних технологій у військову сферу. DIU

працює як венчурний фонд, оминаючи традиційну бюрократію закупівель.

Адаптація в Україні: Український кластер Brave1 є прямою адаптацією моделі DIU. Запуск спільної програми «UNITE – Brave NATO» у 2024 році підтверджує успішність цього підходу. Програма передбачає фінансування спільних розробок українських та західних компаній, що дозволяє інтегрувати українські інновації (перевірені боєм) у стандарти НАТО [16]. Це приклад успішного інституційного запозичення.

Ізраїльська модель публічного управління в сфері оборонних ІТ є еталонною для країни, що перебуває в стані постійної війни. Її основа – інтеграція військової служби з технологічною екосистемою.

Підрозділ 8200 (радіоелектронна розвідка) та елітна навчальна програма «Тальпіот» (Talpiot) є головними драйверами технологічного розвитку Ізраїлю.

– Механізм: Програма «Тальпіот» відбирає 0,1% найкращих призовників, надає їм фундаментальну освіту (фізика, математика, комп'ютерні науки) та інтегрує їх у R&D підрозділи армії на 6-9 років [27].

– Результат: Випускники стають технологічними лідерами, створюючи стартапи після служби («Startup Nation»). Військова служба розглядається не як втрачений час, а як найкращий бізнес-інкубатор [29].

Порівняння з Україною: Україна має потужний людський потенціал, але система мобілізації працює за радянським зразком «заповнення штатних клітинок», а не «управління талантами». Відсутність аналога програми «Тальпіот» призводить до того, що талановиті інженери можуть опинитися в окопах, тоді як армія відчуває дефіцит розробників. Навчальні програми в академіях (наприклад, НГУ) впроваджують DELTA та Кропиву [44], але це навчання користувачів, а не створення архітекторів систем.

Ізраїльський INCD має широкі повноваження, закріплені законодавчо («Cyber Defense Methodology»). У надзвичайних ситуаціях (операція «Залізні мечі») Директорат може видавати обов'язкові до виконання інструкції провайдерам та критичній інфраструктурі [13].

Утримання кадрів: Ізраїльські техногіганти (Microsoft Israel, Wix)

впроваджують спеціальні політики підтримки співробітників під час війни (додаткові відпустки, фінансова допомога), розуміючи, що збереження ментального здоров'я фахівців є запорукою стійкості економіки. В Україні такі практики існують на рівні окремих компаній, але не є частиною державної політики.

Досвід Естонії є найбільш релевантним для України з точки зору побудови «держави у смартфоні» та захисту від російської загрози.

Естонія першою у світі реалізувала концепцію «Посольства даних» (Data Embassy) у Люксембурзі. Це сервери, на яких зберігаються критичні державні реєстри, і які мають статус дипломатичного представництва (суверенна територія Естонії).

– Мета: Забезпечити «цифрову безперервність» (digital continuity). Навіть якщо територія країни буде окупована, уряд зможе функціонувати, виплачувати пенсії, приймати рішення, використовуючи захищену хмарну інфраструктуру за кордоном.

– Правовий аспект: Це вимагало підписання спеціального двостороннього договору, що гарантує недоторканність даних та імунітет від юрисдикції приймаючої країни.

Застосування в Україні: Україна почала рух у цьому напрямку, переносячи резервні копії реєстрів у хмари. Однак, правові бар'єри (юрисдикція, доступ правоохоронних органів) залишаються значними [7]. Реалізація повноцінної моделі Data Embassy вимагає не просто контрактів з Amazon чи Microsoft, а міждержавних угод про імунітет даних.

Естонське кіберкомандування (Cyber Command) інтегроване в структуру Сил оборони, але тісно співпрацює з цивільним сектором та «Кіберлігою захисту» (Cyber Defence League) – добровольчою організацією резервістів-айтішників [4]. Це дозволяє мобілізувати найкращі цивільні уми у кризовий момент без бюрократичної тяганини.

Співпраця з НАТО є стратегічним вектором розвитку української оборонної ІТ-сфери.

Концепція FMN дозволяє об’єднувати системи управління військами різних країн у єдину мережу (Federation) для проведення спільних операцій. Україна активно впроваджує стандарти FMN у систему DELTA.

– Проблеми: Основні виклики лежать не в технологіях, а в процедурах, мовних бар’єрах та стандартах підготовки [18]. НАТО планує розгорнути спеціальну хмарну інфраструктуру для збору даних з поля бою в Україні до 2026 року, що дозволить аналізувати тактику ворога на системному рівні [20].

– Центр передового досвіду (CCDCOE): Приєднання України до CCDCOE у Таллінні як Contributing Participant відкриває доступ до розробки доктрин та участі у навчаннях Locked Shields, що є критичним для синхронізації тактик кіберзахисту [19].

Таблиця 2.2 – Порівняльна таблиця моделей управління

Характеристика	*Модель США (DIU/CISA)*	*Модель Ізраїлю (Talpiot/Unit 8200)*	*Модель Естонії (Data Embassy)*	*Поточний стан України*	*Рекомендована адаптація*
Інноваційний двигун	Комерційні технології -> Армія (Fast-track)	Елітні призовники -> R&D -> Стартапи	Електронне урядування (e-Gov) -> Оборона	Brave1 (Кластерний підхід)	Розширення Brave1 на важку промисловість; спрощення процедур допуску до експлуатації.
Управління талантами	Контрактна армія + Бонуси (проблемні)	Відбір 0.1% кращих (Talpiot), служба в R&D	Добровольчий резерв (Cyber League)	Мобілізація (хаотична), «бронювання» (неефективне)	Впровадження відбору типу «Talpiot» для призовників; створення кадрового резерву IT-фахівців.
Стійкість даних	Розподілені дата-центри	Локальний захист («Залізний купол»)	Data Embassy (Дипломатичний імунітет)	Хмарні бекапи (без статусу посольства)	Підписання міжнародних угод про статус Data Embassy для реєстру «Оберіг» та даних МОУ.
Кібервійська	US CYBERCOM (Окреме командування	Частина розвідки (Unit 8200)	Cyber Command (Частина ЗС)	Створення Кіберсил (Законопроєкт 12349)	Створення окремого роду військ з особливим

	)				статусом комплектування.

Україна здійснила квантовий стрибок у застосуванні ІТ для національної безпеки, перетворившись з об'єкта кіберагресії на суб'єкта, що генерує інновації світового рівня (DELTA, морські дрони, Brave1). Однак, адміністративна надбудова – законодавство, кадрова політика, процедури закупівель – суттєво відстає від технологічних реалій «на землі».

Системні проблеми, такі як фрагментація систем ситуаційної обізнаності, неефективність механізму бронювання ІТ-фахівців та вразливість перед соціальним інжинірингом, вимагають негайних управлінських рішень.

Стратегічні рекомендації для суб'єктів публічного управління:

– Інституціоналізація Кіберсил: Необхідно завершити процес створення Кіберсил як окремого роду військ ЗСУ (відповідно до законопроєкту № 12349 [61]). Ключовим аспектом має стати не техніка, а люди. Слід адаптувати ізраїльську модель відбору та служби, створивши спеціалізовані підрозділи R&D, куди мобілізуватимуть виключно за фаховими навичками, минаючи загальну військову підготовку піхотинця.

– Легалізація «Посольств даних»: Міністерству закордонних справ спільно з Мінцифри та Міноборони ініціювати підписання двосторонніх угод з країнами-партнерами (Польща, Велика Британія, Німеччина) про надання статусу екстериторіальності серверам, що зберігають критичні реєстри України (зокрема «Оберіг»). Це забезпечить юридичний захист суверенітету даних.

– Уніфікація стандартів: РНБО та Міноборони мають затвердити єдиний протокол обміну даними (API) для всіх систем ситуаційної обізнаності (державних та волонтерських). Використання систем, що не підтримують цей стандарт, має бути поетапно обмежене. Запровадження обов'язкової апаратної аутентифікації (ключі FIDO2) для доступу до систем типу DELTA дозволить нівелювати загрозу фішингу.

– Реформа кадрової політики в ІТ: Відмовитися від критеріїв «середньої зарплати» при бронюванні. Замість цього використовувати верифіковану кваліфікацію (сертифікати, досвід, внесок у проєкти Brave1) як

підставу для «технологічної служби». Врахувати помилки США (CISA) та розробити прозору систему фінансової мотивації для кіберфахівців у державному секторі.

Україна має унікальний шанс не просто імплементувати стандарти НАТО, а стати архітектором нових глобальних стандартів цифрової оборони, поєднавши технологічну гнучкість стартапу з інституційною стійкістю держави.

Узагальнюючи міжнародний досвід, варто наголосити, що успішні моделі цифрової безпеки не обмежуються лише технологічними рішеннями чи кадровою політикою, а глибоко інтегровані у зовнішньополітичну діяльність держави через механізми кібердипломатії. Провідні країни світу, зокрема США та Велика Британія, активно використовують інструмент публічної атрибуції кібератак, тобто офіційного покладання відповідальності на конкретну державу або хакерське угруповання. Цей механізм перетворює технічні дані криміналістичного аналізу на юридичні докази, що дозволяє застосовувати санкції та формувати міжнародні коаліції тиску на агресора. Для України, яка часто стає полігоном для випробування новітніх кіберзагроз, опанування цього дипломатичного інструментарію є критично важливим для переведення боротьби з кіберпростору в площину міжнародного права та геополітики.

Окремої уваги заслуговує досвід західних демократій у питанні забезпечення безпеки ланцюгів постачання, відомий як концепція «чистих мереж». Аналіз політики країн Європейського Союзу та США демонструє чітку тенденцію до виключення з національних мереж обладнання та програмного забезпечення, що походить з авторитарних держав або ненадійних юрисдикцій. Це стосується не лише військового сектору, а й телекомунікаційної інфраструктури загалом, як це відбулося з обмеженням технологій 5G від китайських виробників. Для українського публічного управління це слугує сигналом про необхідність перегляду критеріїв державних закупівель, де пріоритетом має стати не найнижча ціна, а довіра до виробника та його незалежність від впливу ворожих спецслужб.

Водночас, імплементація передового досвіду вимагає врахування етичних та правових викликів, з якими вже зіткнулися наші партнери. Зокрема, європейський досвід регулювання штучного інтелекту, втілений у «AI Act», застерігає від безконтрольного використання технологій масового спостереження та автоматизованого прийняття рішень, які можуть загрожувати правам людини. Україна, знаходячись у стані війни, змушена балансувати між потребами безпеки та демократичними цінностями, проте сліпе копіювання інструментів тотального цифрового контролю без належних запобіжників може призвести до розмивання тих самих свобод, які держава захищає на полі бою.

Зрештою, аналіз міжнародних практик підводить до висновку, що найстійкішими виявляються ті системи управління, які змогли побудувати культуру спільної відповідальності за безпеку. У країнах Скандинавії та Балтії ця культура, відома як концепція «тотальної оборони», передбачає, що кібергігієна та цифрова грамотність є базовими навичками кожного громадянина, від школяра до пенсіонера, а не лише вузького кола фахівців. Саме трансформація суспільної свідомості, а не лише закупівля надсучасного обладнання, є тим фундаментом, на якому базується ефективність використання інформаційних технологій у системі національної безпеки провідних держав світу.

Розвиваючи тему міжнародної взаємодії, не можна оминути увагою і кардинальну зміну в суб’єктному складі глобальної безпеки. Сучасний досвід показує, що транснаціональні технологічні корпорації, так звані «Big Tech», фактично перетворилися на геополітичних гравців, чий вплив на національну безпеку інколи співмірний із впливом суверенних держав. У практиці публічного управління США та країн Європи це призвело до появи феномену «технологічної дипломатії», де держава змушена вибудовувати партнерські, а не лише регуляторні відносини з гігантами на кшталт Microsoft, Google чи Amazon. Для української системи управління це відкриває новий напрям діяльності, де посадовці сектору безпеки повинні володіти навичками переговорів з корпоративним сектором, оскільки саме у хмарних сховищах та

на серверах цих компаній часто вирішується доля критично важливих даних та стабільність цифрових послуг.

Варто також детальніше зупинитися на міжнародних підходах до фінансування оборонних інновацій, які докорінно відрізняються від традиційних бюджетних процедур. У країнах НАТО набуває поширення модель, коли державні оборонні відомства виступають у ролі венчурних інвесторів. Створюючи спеціалізовані фонди або інноваційні хаби, держава вкладає кошти в технологічні стартапи на ранніх етапах розвитку, розділяючи з ними ризики заради отримання унікальних технологічних переваг у майбутньому. Такий підхід дозволяє обійти неповороткість класичних державних закупівель і дає змогу швидко інтегрувати рішення подвійного призначення, розроблені цивільним сектором, у військову сферу, що є критично важливим уроком для реформування української системи оборонного замовлення.

Ще одним важливим аспектом, який варто перейняти з міжнародної практики, є стандартизація процесів обміну даними, відома як інтероперабельність. У межах НАТО це поняття виходить далеко за рамки технічної сумісності радіостанцій чи комп’ютерних мереж; це передусім управлінська філософія, що передбачає єдині протоколи розуміння ситуації та прийняття рішень. Західний досвід демонструє, що ефективна коаліційна безпека можлива лише тоді, коли національні системи управління здатні «спілкуватися» однією цифровою мовою без необхідності додаткових адаптерів чи ручного перенесення даних. Для України це означає, що будь-яка національна ІТ-система, яка розробляється сьогодні, повинна апріорі створюватися з архітектурою, відкритою для інтеграції з системами партнерів.

Крім того, слід звернути увагу на еволюцію підходів до підготовки кадрів у провідних країнах світу. Традиційні академічні лекції дедалі більше поступаються місцем практичним тренуванням на кіберполігонах, або так званим «кіберрейнджам». Це віртуальні середовища, які дозволяють моделювати реальні атаки на інфраструктуру – від злому електростанції до

витоку фінансових даних – і відпрацьовувати командну взаємодію в режимі реального часу. У міжнародній практиці такі навчання часто проводяться спільно представниками державного та приватного секторів, що дозволяє виявити слабкі місця в комунікації та процедурах реагування ще до настання реальної кризи, перетворюючи помилки на навчальний матеріал, а не на причину катастрофи.

Досліджуючи міжнародні практики, неможливо оминути увагою і такий специфічний управлінський інструмент, як національні центри обробки даних розвідки, або так звані «fusion centers». Досвід Сполучених Штатів та країн Європейського Союзу свідчить, що ефективна протидія сучасним загрозам вимагає відмови від відомчого егоїзму, коли кожна спецслужба накопичує інформацію виключно для себе. Сучасна філософія публічного управління у цій сфері базується на принципі «need to share» замість застарілого «need to know». Це означає створення єдиних аналітичних хабів, де представники різних відомств – від поліції до військової розвідки та аналітиків фінансового моніторингу – працюють в одному фізичному та цифровому просторі, що дозволяє виявляти неочевидні зв’язки між кібератаками, фінансуванням тероризму та дезінформаційними кампаніями.

Окрім технічного та розвідувального аспектів, передовий міжнародний досвід демонструє зміну підходів до захисту когнітивного простору громадян. Якщо раніше інформаційна безпека асоціювалася переважно із захистом технічних каналів зв’язку, то нині провідні держави інвестують значні ресурси в технології виявлення та нейтралізації ворожих наративів ще на етапі їх зародження. Зокрема, у практиці публічного управління країн Балтії та Великої Британії активно застосовується концепція стратегічних комунікацій, яка передбачає не пасивне спростування фейків, а проактивне наповнення інформаційного простору власним порядком денним. Для цього використовуються складні системи моніторингу соціальних мереж на основі штучного інтелекту, які дозволяють фіксувати аномальну активність ботоферм і реагувати на неї автоматизовано, не чекаючи ручного втручання операторів.

Також варто згадати про еволюцію нормативно-правового регулювання так званої «активної оборони». У світовій практиці все гучніше лунають дискусії про право держави не лише відбивати кібератаки на своїй території, а й проводити превентивні дії в мережах противника. Сполучені Штати та Велика Британія поступово легалізують доктрину, яка дозволяє їхнім кібервійськам порушувати роботу інфраструктури хакерських угруповань ще до того, як ті завдадуть удару. З точки зору теорії публічного управління, це створює складну дилему, адже межа між активною обороною та актом агресії в цифровому просторі є вкрай тонкою, що вимагає розробки нових протоколів прийняття рішень на найвищому політичному рівні та чітких механізмів парламентського контролю за такими операціями.

Завершуючи огляд інструментарію, слід звернути увагу на те, як розвинені країни вирішують проблему цифрової ідентифікації громадян, що є наріжним каменем безпеки електронних послуг. Досвід Естонії та скандинавських країн показує, що національна система цифрового ID (Mobile ID, Smart-ID) є не просто сервісом зручності, а елементом національної безпеки. Вона дозволяє однозначно верифікувати особу в цифровому просторі, унеможливлюючи анонімні маніпуляції та шахрайство. Для системи публічного управління це означає необхідність побудови такої інфраструктури довіри, де держава виступає гарантом ідентичності, але при цьому забезпечує повну конфіденційність персональних даних, не допускаючи їх компрометації.

РОЗДІЛ 3
ШЛЯХИ ВДОСКОНАЛЕННЯ ПУБЛІЧНОГО УПРАВЛІННЯ ПРОЦЕСАМИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ІНТЕРЕСАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

3.1 Стратегічні напрями оптимізації державної політики щодо використання ІТ для нейтралізації гібридних загроз

Сучасна геополітична ситуація, що характеризується безпрецедентним рівнем турбулентності та гібридними загрозами, ставить перед Україною екзистенційні виклики, відповідь на які лежить не лише у площині військової доблесті, але й у сфері управлінської ефективності. Повномасштабна агресія Російської Федерації стала каталізатором фундаментальних змін у парадигмі національної безпеки, де інформаційні технології (ІТ) перетворилися з допоміжного інструменту на основний домен ведення бойових дій. Війна дронів, кібернетичні атаки на критичну інфраструктуру, використання штучного інтелекту для аналізу розвідувальних даних та автоматизовані системи управління військами (C4ISR) – це нова реальність, яка вимагає від системи публічного управління адаптивності, швидкості та інноваційності.

Для глибокого розуміння проблематики необхідно чітко розмежувати поняття «державне управління» та «публічне управління» (public governance), оскільки ця термінологічна різниця відображає сутнісний зсув у підходах до забезпечення безпеки. Традиційне державне управління базується на монополії держави на застосування сили та прийняття рішень, характеризується директивністю та закритістю. Натомість публічне управління розглядає безпеку як суспільне блага, у створенні якого беруть участь різноманітні актори: органи державної влади, місцеве самоврядування, бізнес-структури, наукові установи та громадянське суспільство.

В умовах України цей перехід став не теоретичною конструкцією, а практичною необхідністю. З початком повномасштабного вторгнення саме механізми публічного управління дозволили мобілізувати ресурси нації. Приватні ІТ-компанії взяли на себе функції кіберзахисту державних реєстрів, волонтерські групи забезпечували підрозділи зв'язком Starlink, а розрізнені групи розробників почали створювати програмне забезпечення для артилерії («Кропива», «GIS Arta»). Як зазначають дослідники, відмінність механізмів публічного управління полягає у залученні широкого кола стейкхолдерів для виконання функцій, які раніше вважалися виключною прерогативою спецслужб та військових [45].

Управління процесами використання ІТ в інтересах нацбезпеки сьогодні включає такі ключові компоненти:

– Інституційний компонент: Сукупність органів влади та неурядових організацій.

– Нормативно-правовий компонент: Законодавче поле, що регулює кібербезпеку, оборонні закупівлі та захист інформації.

– Технологічний компонент: Інфраструктура, стандарти передачі даних, платформи взаємодії.

– Соціокультурний компонент: Рівень цифрової грамотності, культура безпеки та довіра між учасниками процесу.

Фундамент системи управління закладено у Конституції України, Законі «Про національну безпеку України» та Стратегії кібербезпеки України. Аналіз цих документів свідчить про поступове усвідомлення законодавцем важливості цифрової складової. Зокрема, Стратегія кібербезпеки визначає кіберпростір як одну з сфер ведення бойових дій. Проте, на практиці існує суттєвий розрив (gap) між декларативними нормами стратегій та підзаконними актами, що регулюють щоденну діяльність.

Критичним аспектом є правове регулювання захисту критичної інформаційної інфраструктури (КІІ). Чинне законодавство покладає відповідальність на власників об'єктів КІІ, однак механізми державного

контролю та допомоги часто залишаються забюрократизованими. Існує проблема застарілості нормативної бази у сфері технічного захисту інформації (ТЗІ), яка базується на стандартах 90-х років (система КСЗІ) і не відповідає динаміці сучасних кіберзагроз [62].

Окремим блоком стоїть питання законодавчого забезпечення гібридної протидії. Як вказують аналітики, законодавство ЄС та країн НАТО (наприклад, Cyber Resilience Act) рухається у бік «безпеки дизайну» (security by design) та відповідальності виробників програмного забезпечення. Українське ж законодавство досі сфокусоване на «паперовій» відповідності атестатам, що створює бар'єри для впровадження інновацій [33].

Система управління національною безпекою в ІТ-сфері є поліцентричною, що має як переваги (стійкість, відсутність єдиної точки відмови), так і недоліки (дублювання функцій, конкуренція відомств).

1. Рада національної безпеки і оборони України (РНБО) та НКЦК.

Національний координаційний центр кібербезпеки (НКЦК) при РНБО виступає головним стратегічним хабом. Згідно з Положенням, рішення НКЦК є обов'язковими для розгляду всіма органами влади [66]. Центр має повноваження ініціювати введення надзвичайного стану у разі масованих кібератак, здійснювати атрибуцію агресії та координувати міжнародну співпрацю. Важливим аспектом є функція НКЦК щодо аналізу кіберінцидентів на предмет їх кваліфікації як збройної агресії відповідно до норм міжнародного права [56]. Це критично важливо для задіяння механізмів колективної оборони (наприклад, статті 5 Статуту НАТО в перспективі).

2. Міністерство цифрової трансформації України (Мінцифра).

Мінцифра вийшла за межі класичного «сервісного» міністерства і стала ключовим гравцем у сфері оборонних інновацій. Через проекти «Армія дронів» та екосистему «Дія», міністерство фактично реалізує функцію технолога національної безпеки. Мінцифра просуває концепцію «Цифрової держави» (Digital State), яка в умовах війни трансформується у «Agent State» – державу, що проактивно діє в інтересах громадян та оборони [22].

3. Міністерство оборони України (МОУ) та Збройні Сили України (ЗСУ).

МОУ виступає основним замовником та формує політики у сфері оборони. ЗСУ є кінцевим споживачем технологій. Проблемою залишається складна процедура передачі розробок від волонтерів на баланс ЗСУ, хоча постанова Кабміну №345 значно спростила цей процес. Створення нових агенцій – Агенції оборонних закупівель (АОЗ) та Державного оператора тилу (ДОТ) – має на меті розмежувати функції формування політики та її реалізації (закупівель), що відповідає стандартам НАТО [65].

4. Спеціальні служби (СБУ, Держспецзв'язку).

СБУ фокусується на контррозвідувальному захисті та боротьбі з кібертероризмом. Держспецзв'язку відповідає за захист державних інформаційних ресурсів та урядовий зв'язок. Взаємодія між цими структурами не завжди є ідеальною через різні підходи до безпеки: СБУ орієнтована на оперативну роботу, а Держспецзв'язку – на нормативну та технічну.

Однією з ключових проблем є відсутність єдиної архітектури даних сектору безпеки і оборони. Різні відомства створюють власні реєстри та системи ситуаційної обізнаності, які часто не сумісні між собою. Це призводить до фрагментації інформаційного простору та ускладнює прийняття управлінських рішень.

Наприклад, система управління логістикою ЗСУ може не мати автоматизованого обміну даними з митними реєстрами, що уповільнює ввезення комплектуючих для дронів. Або ж системи кібермоніторингу НКЦК та CERT-UA (команда реагування на комп'ютерні надзвичайні події при Держспецзв'язку) можуть дублювати функції моніторингу мережевого трафіку.

Створення кластеру оборонних технологій Brave1 стало інституційною відповіддю на потребу швидкої інтеграції цивільних розробок у військову сферу. Це унікальний приклад публічно-приватного партнерства, засновниками якого виступили Мінцифра, Міноборони, Генштаб, РНБО, Мінекономіки та Мінстратегпром.

Brave1 позиціонується як «єдине вікно» для інноваторів. Механізм роботи полягає у наступному:

– Подача заявки: Розробник подає ідею або прототип через портал.

– Військова експертиза: Генштаб оцінює актуальність розробки для фронту.

– Грантова підтримка: Проекти отримують безповоротне фінансування ($5k, $30k, і тепер більше) на розвиток.

– Допуск до експлуатації: Кластер супроводжує процес кодифікації та випробувань.

За даними звітів, Україна збільшила виробництво оборонної продукції у 35 разів з 2022 року, що значною мірою є заслугою спрощених процедур, запроваджених через екосистему Brave1 [65].

Окрім роботи зі стартапами, кластер запустив ініціативу Brave1 Club для зрілих компаній, які не потребують грантів, але потребують організаційної підтримки. Це механізм консолідації лідерів ринку для координації R&D та створення спільних підприємств. Учасники клубу отримують пріоритетний доступ до полігонних випробувань, прямий зв’язок з бойовими підрозділами (feedback loop) та можливість презентувати продукцію на міжнародних майданчиках [43].

Такий підхід свідчить про еволюцію управління: від простого розподілу коштів до створення екосистеми підтримки, що включає нетворкінг, менторство та інвестиційний консалтинг. Це наближає українську модель до західних акселераторів, проте залишається проблема залежності від державного або донорського фінансування.

Попри успіхи, модель Brave1 має системні обмеження:

– Правовий статус: Brave1 де-юре не є окремим органом влади, а функціонує як спільний проект. Це створює ризики інституційної нестійкості у разі зміни політичного керівництва.

– Інтелектуальна власність: Найбільш болючим питанням залишається захист прав інтелектуальної власності (ІВ). Українські стартапи,

навіть отримавши грант від Brave1, часто реєструють основну компанію (Headquarters) за кордоном (Делавер, Естонія, Кіпр) для залучення венчурних інвестицій. Це призводить до того, що юридично технології стають іноземними, а Україна ризикує перетворитися на «складальний цех» та полігон, втрачаючи права на високомаржинальні продукти [34].

– Відсутність «довгих» грошей: Гранти покривають початкові стадії (Pre-seed), але для масштабування виробництва потрібні мільйонні інвестиції або довгі державні контракти, механізм яких досі забюрократизований.

Досвід Ізраїлю є найбільш релевантним для України, зважаючи на схожість екзистенційних загроз. Центральним елементом ізраїльської системи є DDR&D (Directorate of Defense Research and Development), відомий на івриті як Mafat.

Організаційна структура та статус: Mafat має унікальний статус «подвійного підпорядкування»: його керівник звітує одночасно Генеральному директору Міністерства оборони та Начальнику Генерального штабу ЦАХАЛ. Це усуває розрив між адміністраторами бюджету та військовими, які воюють. Mafat відповідає за весь цикл: від фундаментальних досліджень до повномасштабної розробки (FSD) та закупівель.

Механізми взаємодії зі стартапами: На відміну від традиційного держзамовлення, Mafat створив гнучкі інструменти спільно з Ізраїльським управлінням інновацій (IIA):

– Програма «Meimad»: Спільний фонд для технологій подвійного призначення. Фінансує R&D на стадії TRL 3-5 (Technology Readiness Level). Держава бере на себе 50-90% ризиків.

– Акселератор «Innofense»: Програма для стартапів ранніх стадій. Компанії отримують грант (близько $50-60k), менторство та доступ до баз даних ЦАХАЛ, при цьому повністю зберігаючи права на інтелектуальну власність.

– Залучення венчурного капіталу: У 2025 році Ізраїль запустив механізм державних гарантій (200 млн шекелів) для венчурних фондів, що

інвестують у Defense Tech. Це стимулює приватних інвесторів вкладати у ризиковані оборонні проекти [28].

Культура цифрової компетентності: Ізраїльська екосистема базується на високій цифровій грамотності населення та «плоских» ієрархіях. Як зазначають оглядачі, українська культура також нагадує «хакерський колектив», де рішення приймаються швидко через месенджери (Signal, WhatsApp), що ріднить нас з ізраїльським підходом. Однак, в Ізраїлі ця культура інституціоналізована через систему призову (підрозділ 8200), яка постачає кадри для стартапів [24].

Співпраця з НАТО вимагає від України не лише технічної сумісності, але й управлінської. Огляд НАТО щодо українських закупівельних агенцій містить критично важливі рекомендації [65]:

– Заборона радикальних змін під час війни: НАТО прямо рекомендує (Рекомендація №1) утриматися від повної централізації закупівель та злиття АОЗ і ДОТ до завершення воєнного стану, щоб не зруйнувати існуючі ланцюги постачання.

– Розрахунок вартості життєвого циклу (LCC): Перехід від критерію «найнижча ціна» до оцінки сукупної вартості володіння (розробка + експлуатація + утилізація). Для ІТ-систем це критично, адже підтримка софту часто дорожча за його написання.

– Інтеграція в процес планування: Закупівельні агенції повинні бути залучені до процесу формування технічних вимог, а не просто виконувати заявки Генштабу (Рекомендація №5).

Ініціатива NATO-Ukraine «Unite Brave» та проведення спільних хакатонів демонструють готовність Альянсу інтегрувати українські інновації, проте бюрократичні процедури НАТО залишаються складними для українських малих компаній [50].

Виходячи з проведеного аналізу міжнародного досвіду та поточного стану справ, стратегічним пріоритетом оптимізації державної політики має стати перехід від ситуативного реагування до системного управління

архітектурою національної стійкості. Першочерговим завданням у цьому контексті є юридичне врегулювання статусу «цифрових активів» у секторі оборони. Наявна нормативна база, що регулює постановку озброєння на баланс, досі оперує категоріями матеріального світу, де програмне забезпечення розглядається як додаток до «заліза». Це створює колізії, коли оновлення коду бойової системи вимагає проходження тих самих бюрократичних процедур, що й модернізація танку. Тому оптимізація політики вимагає запровадження спеціального правового режиму для Military Tech, який дозволив би легалізувати використання програмних продуктів на етапі їх тестування в реальних бойових умовах, застосувуючи принцип «regulatory sandbox» або регуляторної пісочниці.

Наступним стратегічним вектором є вирішення проблеми інтероперабельності, тобто здатності різних систем до взаємодії. Державна політика не повинна намагатися створити одну «супер-систему», яка замінить усі існуючі, оскільки це шлях до монополізації та вразливості. Натомість, зусилля публічного управління мають бути спрямовані на затвердження єдиних протоколів обміну даними. Держава має виступати не як «головний програміст», а як архітектор стандартів, вимагаючи від усіх розробників – чи то державних підприємств, чи то волонтерських груп – дотримання єдиних правил API (інтерфейсів прикладного програмування). Тільки так можна уникнути «цифрового феодалізму», коли кожен рід військ користується власною, закритою від інших системою ситуаційної обізнаності.

Невід’ємною складовою стратегії має стати і питання цифрового суверенітету в контексті використання хмарних технологій. Оскільки фізичне знищення дата-центрів в Україні залишається реальною загрозою, перенесення державних реєстрів та військових баз даних у закордонні хмари є безальтернативним. Однак це вимагає кардинально нових рішень у сфері міжнародного права. Україні необхідно ініціювати підписання міжурядових угод про створення «цифрових посольств», які б гарантували, що сервери з українськими даними на території країн-партнерів мають той самий

дипломатичний імунітет, що й територія звичайного посольства. Це дозволить убезпечити критичну інформацію від доступу іноземних юрисдикцій чи комерційних суперечок.

Окремої уваги потребує трансформація кадрової політики як складової державного управління. Стратегічний підхід вимагає відмови від радянської моделі комплектування ІТ-підрозділів за залишковим принципом. Необхідно впровадити диференційовану систему мобілізації, яка б дозволяла залучати фахівців цивільного сектору до виконання специфічних завдань кіберзахисту без відриву від виробництва або в форматі служби в спеціалізованих кіберцентрах. Державна політика має визнати, що інженер, який налаштовує системи радіоелектронної боротьби або захищає периметр енергомережі, робить для оборони не менше, ніж солдат на передовій, і це має бути відображено в нормах бронювання та соціального забезпечення.

Врешті-решт, стратегія використання ІТ для нейтралізації гібридних загроз має базуватися на принципі довіри до приватного сектору. Держава повинна делегувати частину функцій кібермоніторингу та розробки програмного забезпечення перевіреним приватним компаніям, залишаючи за собою функції контролю та стратегічного планування. Це дозволить подолати неповороткість державного апарату та забезпечити постійний притік інновацій, необхідних для перемоги у технологічній війні.

Розвиваючи тему економічної складової державної політики, варто наголосити, що оптимізація публічного управління неможлива без перегляду підходів до фінансування оборонних інновацій. Нинішня модель, яка значною мірою спирається на волонтерський ресурс та обмежені державні гранти, є ефективною для тактичного реагування, але недостатньою для довгострокового стратегічного розвитку. Держава повинна створити умови для приходу в цей сектор приватного венчурного капіталу, зокрема іноземного. Це вимагає від органів влади розробки прозорих механізмів страхування воєнних ризиків для інвесторів, які готові вкладати кошти в український Military Tech. Без державних гарантій захисту інвестицій ми ризикуємо залишитися на рівні

кустарного виробництва, тоді як ворог індустріалізує свої технологічні процеси.

Водночас, стратегічним напрямом має стати реформа системи експортного контролю. Це може здаватися парадоксальним в умовах війни, коли все озброєння потрібне на фронті, але повна заборона експорту оборонних технологій знекровлює виробників. Публічне управління тут має знайти тонкий баланс: дозволити компаніям продавати свої рішення союзникам для отримання валютної виручки, яку вони зможуть реінвестувати в нові розробки (R&D), при цьому жорстко контролюючи нерозповсюдження критичних технологій. Тобто держава має перетворитися з «цербера», що забороняє все, на регулятора, який допомагає українським компаніям заробляти на світових ринках, аби вони могли краще озброювати власну армію.

Ще одним важливим вектором оптимізації є зміна підходу до роботи з інтелектуальною власністю в оборонній сфері. Наразі існує страх розробників передавати технічну документацію державі через ризик витоку інформації або втрати прав на продукт. Оптимізація політики передбачає запровадження зрозумілих ліцензійних угод, де держава виступає гарантованим замовником, але залишає майнові права за винахідником. Це стимулюватиме конкуренцію та інновації, адже розробник буде зацікавлений у постійному вдосконаленні продукту, знаючи, що це його актив.

Крім того, необхідно звернути увагу на науково-освітній аспект державної політики. Оптимізація тут полягає у відході від абстрактного викладання технічних дисциплін до створення на базі університетів закритих дослідницьких кластерів, які працюють над реальними завданнями сектору безпеки. Держава має сформувати замовлення не лише на готовий продукт, а й на прикладні дослідження у сфері штучного інтелекту, радіоелектронної боротьби та криптографії, надаючи науковцям доступ до деперсоніфікованих даних з поля бою. Тільки поєднавши фундаментальну науку з реальними потребами фронту, ми зможемо забезпечити технологічну перевагу не на місяці, а на роки вперед.

3.2 Вдосконалення організаційно-правового механізму впровадження сучасних ІТ в систему нацбезпеки

Ситуація з правами на ІВ у сфері Defense Tech є загрозливою.

Суть проблеми: Українське законодавство та судова практика не забезпечують належного захисту прав інвесторів та винахідників. Реєстрація торгової марки в Україні може тривати до 1.5-2 років, а механізми захисту від патентного тролінгу є слабкими [73]. Вищий суд з питань інтелектуальної власності, передбачений реформою 2017 року, досі не запрацював [63].

Наслідки: Стартапи, що розробляють критичні технології (ШІ-наведення, системи РЕБ), масово інкорпоруються в іноземних юрисдикціях. Інвестори вимагають передачі прав на ІВ компаніям у США або ЄС як умову фінансування. Як наслідок, Україна втрачає податкові надходження та контроль над технологіями. Засновник компанії TAF Industries зазначає: «Частина deftech-компаній уже перестали бути українськими» [34]. Це створює загрозу, що після війни Україна буде змушена купувати власні ж розробки у іноземних правовласників.

Вимога побудови Комплексної системи захисту інформації (КСЗІ) для державних інформаційних ресурсів перетворилася на гальмо прогресу.

– Проблема: Процедура атестації КСЗІ є тривалою, дороговартісною та орієнтованою на статичні системи. У світі хмарних технологій та мікросервісної архітектури, де оновлення коду відбуваються щодня, концепція КСЗІ (яка «фіксує» стан системи) є технічно неспроможною.

– Конфлікт стандартів: Замовники у тендерах часто вимагають сертифікат КСЗІ, ігноруючи міжнародні стандарти ISO 27001. Антимонопольний комітет (АМКУ) у своїй практиці часто стає на бік формальних вимог замовника, що блокує участь у тендерах компаній, які мають сучасні системи захисту, але не мають паперового атестату Держспецзв’язку [64].

– Хмарні послуги: Закон «Про хмарні послуги» дозволив використання хмар для публічного сектору, але підзаконні акти все ще вимагають складних процедур підтвердження відповідності для систем, що обробляють службову інформацію [62].

Управління високотехнологічною безпекою вимагає нових компетентностей. Стандарт вищої освіти за спеціальністю 281 «Публічне управління та адміністрування» (магістр), затверджений у 2020 році, хоч і є кроком вперед, але не містить чітких вимог щодо цифрової безпеки та управління Defense Tech проектами [58].

Дослідження вказують на необхідність формування у державних службовців не лише «soft skills», а й специфічних навичок роботи в умовах кіберагресії, розуміння етики використання ШІ та управління ризиками [46]. Відсутність таких фахівців призводить до того, що технічні завдання на розробку систем пишуться неякісно, а прийняті системи не відповідають потребам користувачів.

На основі проведеного аналізу пропонується комплексна стратегія реформування системи публічного управління у досліджуваній сфері.

Необхідно трансформувати кластер Brave1 у повноцінну державну інституцію – Агенцію оборонних досліджень та інновацій, побудовану за зразком ізраїльського Mafat.

– Статус: Центральний орган виконавчої влади зі спеціальним статусом.

– Підпорядкування: Подвійне – Міністру оборони (оперативний контроль) та Віце-прем’єру з інновацій (стратегічний розвиток).

– Функції: Не лише видача грантів, а й управління повним життєвим циклом інновацій, включаючи формування довгострокових R&D контрактів, які наразі відсутні в правовому полі України.

– Фінансові інструменти: Надання державних гарантій для приватних венчурних фондів, що інвестують в український Deep Tech, знижуючи їх ризики (за прикладом Ізраїлю) [28].

Для зупинки «витоку мізків» та технологій необхідно впровадити спеціальний режим для оборонних інновацій:

– Затвердити модель, за якою держава фінансує розробку через гранти, але залишає 100% майнових прав на ІВ за розробником. Натомість держава отримує безоплатну, безвідкличну ліцензію на використання продукту для потреб ЗСУ (Government Purpose Rights), як це працює в США та Ізраїлі [21]. Це дозволить стартапам капіталізувати свій актив та залучати інвесторів, не боячись втратити бізнес.

– Впровадити податковий режим, що передбачає знижену ставку податку на прибуток, отриманий від використання об’єктів інтелектуальної власності, зареєстрованих в Україні.

– Створити механізм депонування вихідного коду критичного ПЗ у державному репозиторії. Якщо розробник банкрутує або зникає, держава отримує доступ до коду для підтримки системи, але за нормальних умов не втручається у бізнес.

Необхідна докорінна зміна підходу до ТЗІ:

– Скасування тотальної КСЗІ: Обмежити вимогу побудови КСЗІ лише системами, що обробляють інформацію, яка становить державну таємницю. Для решти систем (включаючи службову інформацію) запровадити декларування відповідності стандартам ISO/IEC 27001 та NIST [62].

– Risk Management Framework: Впровадити обов’язкову процедуру регулярної оцінки ризиків та тестувань на проникнення (pentesting) як основу підтвердження безпеки. Безпека – це процес, а не стан.

– Відповідальність постачальників: Законодавчо закріпити відповідальність розробників ПЗ за виявлені вразливості та зобов’язання їх виправляти (SLA на безпеку).

Централізація з розумом: Виконати рекомендацію НАТО щодо утримання від злиття АОЗ та ДОТ до кінця війни, зосередившись на розбудові їх спроможностей [65].

Уніфікація каталогів: Прискорити впровадження натівської системи

кодифікації для всіх видів ІТ-продукції. Це дозволить українським виробникам автоматично потрапляти у каталоги постачальників Альянсу.

Закупівля «capability»: Переходити від закупівлі «штук» (дронів, радіостанцій) до закупівлі «спроможностей» (забезпечення відеоспостереження на ділянці фронту). Це дозволить постачальникам пропонувати комплексні сервісні рішення, а не просто «залізо».

Оновлення освітніх стандартів: Внести зміни до стандарту спеціальності 281 «Публічне управління та адміністрування», додавши компетентності: «Управління цифровими проектами у публічному секторі», «Основи національної кіберстійкості», «Правове регулювання штучного інтелекту».

CDTO у силових відомствах: Запровадити посади заступників з цифрової трансформації (CDTO) на рівні бригад та регіональних управлінь силових структур. Це забезпечить вертикаль впровадження інновацій «знизу-вгору».

Бронювання інженерів: Розробити прозорий механізм бронювання ключових технічних фахівців приватних Defense Tech компаній, базуючись на їх реальному внеску в обороноздатність, а не лише на розмірі сплачених податків.

Система публічного управління національною безпекою України перебуває у стані активної трансформації. Війна виявила нежиттєздатність старих бюрократичних підходів та стимулювала появу унікальних механізмів, таких як екосистема Brave1 та цифрові інструменти Мінцифри.

Однак, для досягнення стійкої технологічної переваги над ворогом необхідно вирішити низку системних проблем: подолати правовий нігілізм у сфері інтелектуальної власності, відмовитися від застарілої системи КСЗІ на користь ризик-орієнтованих підходів та гармонізувати процедури закупівель зі стандартами НАТО.

Реалізація запропонованої моделі – створення Агенції оборонних інновацій за ізраїльським зразком, захист прав розробників та інвестиції в людський капітал – дозволить перетворити Україну з імпортера безпекових рішень на глобального донора безпеки та технологічного лідера у сфері Defense

Tech. Це не лише питання перемоги у війні, а й питання майбутнього місця України у світовій архітектурі безпеки.

Окрім вирішення питань інтелектуальної власності та сертифікації, вдосконалення організаційно-правового механізму вимагає перегляду самої філософії поводження з даними як стратегічним активом. Чинна система класифікації інформації з обмеженим доступом, яка дісталася нам у спадок від радянських часів, є надмірно громіздкою і часто стає на заваді оперативному обміну розвідувальними даними з партнерами. Тому нагальним завданням є гармонізація національних грифів секретності зі стандартами НАТО, що дозволить створити єдиний довірений простір обміну інформацією. Це передбачає внесення змін до Закону України «Про державну таємницю» в частині чіткого розмежування інформації, яка дійсно потребує найвищого ступеня захисту, та інформації, яка може оброблятися в автоматизованих системах класу «Restricted» без надмірних бюрократичних обмежень.

Логічним продовженням цього процесу має стати законодавче врегулювання статусу цифрових активів у секторі оборони, адже на сьогоднішній день програмне забезпечення, що використовується для управління вогнем чи логістикою, часто не має чіткого правового визначення як озброєння. Це створює парадоксальні ситуації, коли закупити «залізо» простіше, ніж ліцензію на софт, від якого залежить ефективність цього заліза. Оновлений механізм має передбачати спрощені процедури обліку, списання та модернізації нематеріальних активів, визнаючи код повноцінною зброєю, яка потребує постійного обслуговування та вдосконалення.

Важливим елементом правової реформи є також лібералізація системи експортного контролю для технологій подвійного призначення. В умовах, коли межа між цивільним дроном і бойовим засобом ураження фактично стерта, жорсткі обмеження на трансфер технологій можуть гальмувати розвиток галузі та позбавляти українських виробників можливості конкурувати на зовнішніх ринках. Організаційно-правовий механізм повинен трансформуватися від заборонного до контрольно-дозволеного, де держава не блокує експорт, а

супроводжує його, забезпечуючи дотримання міжнародних зобов'язань України щодо нерозповсюдження зброї масового знищення, але не перешкоджаючи комерційному успіху вітчизняних ІТ-компаній.

Окремої уваги потребує нормативне закріплення процедур так званої «швидкої легалізації» бойового досвіду, коли зміни до тактичних настанов та бойових статутів вносяться не роками, а в режимі реального часу на основі аналізу даних з поля бою. Сучасні інформаційні технології дозволяють збирати та аналізувати ці дані миттєво, проте чинна нормативна база вимагає тривалих погоджень для затвердження нових алгоритмів дій підрозділів. Створення гнучкого правового механізму, який дозволяв би командувачам родів військ самостійно затверджувати тимчасові інструкції на основі цифрового моделювання ситуацій, значно підвищило б адаптивність системи управління до динамічних змін обстановки.

Окрім вирішення питань інтелектуальної власності та сертифікації, вдосконалення організаційно-правового механізму вимагає перегляду самої філософії поводження з даними як стратегічним активом. Чинна система класифікації інформації з обмеженим доступом, яка дісталася нам у спадок від радянських часів, є надмірно громіздкою і часто стає на заваді оперативному обміну розвідувальними даними з партнерами. Тому нагальним завданням є гармонізація національних грифів секретності зі стандартами НАТО, що дозволить створити єдиний довірений простір обміну інформацією. Це передбачає внесення змін до Закону України «Про державну таємницю» в частині чіткого розмежування інформації, яка дійсно потребує найвищого ступеня захисту, та інформації, яка може оброблятися в автоматизованих системах класу «Restricted» без надмірних бюрократичних обмежень.

Логічним продовженням цього процесу має стати законодавче врегулювання статусу цифрових активів у секторі оборони, адже на сьогоднішній день програмне забезпечення, що використовується для управління вогнем чи логістикою, часто не має чіткого правового визначення як озброєння. Це створює парадоксальні ситуації, коли закупити «залізо»

простіше, ніж ліцензію на софт, від якого залежить ефективність цього заліза. Оновлений механізм має передбачати спрощені процедури обліку, списання та модернізації нематеріальних активів, визнаючи код повноцінною зброєю, яка потребує постійного обслуговування та вдосконалення.

Важливим елементом правової реформи є також лібералізація системи експортного контролю для технологій подвійного призначення. В умовах, коли межа між цивільним дроном і бойовим засобом ураження фактично стерта, жорсткі обмеження на трансфер технологій можуть гальмувати розвиток галузі та позбавляти українських виробників можливості конкурувати на зовнішніх ринках. Організаційно-правовий механізм повинен трансформуватися від заборонного до контрольно-дозволеного, де держава не блокує експорт, а супроводжує його, забезпечуючи дотримання міжнародних зобов'язань України щодо нерозповсюдження зброї масового знищення, але не перешкоджаючи комерційному успіху вітчизняних IT-компаній.

Окремої уваги потребує нормативне закріплення процедур так званої «швидкої легалізації» бойового досвіду, коли зміни до тактичних настанов та бойових статутів вносяться не роками, а в режимі реального часу на основі аналізу даних з поля бою. Сучасні інформаційні технології дозволяють збирати та аналізувати ці дані миттєво, проте чинна нормативна база вимагає тривалих погоджень для затвердження нових алгоритмів дій підрозділів. Створення гнучкого правового механізму, який дозволяв би командувачам родів військ самостійно затверджувати тимчасові інструкції на основі цифрового моделювання ситуацій, значно підвищило б адаптивність системи управління до динамічних змін обстановки.

Узагальнюючи викладене, можна стверджувати, що вдосконалення організаційно-правового механізму є не просто технічним корегуванням законодавства, а фінальним етапом тієї зміни управлінської парадигми, про яку йшлося на початку нашого дослідження. Ми бачимо чітку еволюцію: якщо теоретично ми розглядали перехід від захисту периметра до кіберстійкості, а на практиці спостерігали, як волонтерський хаос трансформується в інноваційні

екосистеми на кшталт Brave1, то саме оновлене правове поле має стати тим каркасом, що зафіксує ці незворотні зміни. Система публічного управління національною безпекою перестає бути монолітною вертикаллю, перетворюючись на гнучку мережу, де держава виступає не стільки командиром, скільки архітектором та гарантом правил гри.

Ключовим висновком з аналізу всіх аспектів – від проблем з інтелектуальною власністю до питань інтероперабельності з НАТО – є те, що ефективність цифрової зброї залежить не лише від якості коду, а й від якості управлінських рішень, які супроводжують її створення та застосування. Легалізація нових підходів до секретності, впровадження ризик-орієнтованих методів сертифікації та відмова від застарілих бюрократичних процедур – це той необхідний фундамент, без якого навіть найсучасніші технології залишаться локальними експериментами, а не системним фактором перемоги.

Таким чином, успішна імплементація запропонованих організаційно-правових змін дозволить Україні вирішити подвійне завдання: в короткостроковій перспективі – забезпечити технологічну перевагу на полі бою за рахунок швидкості та адаптивності, а в довгостроковій – інтегруватися у глобальну архітектуру безпеки як повноправний суб’єкт, що володіє унікальним досвідом управління гібридними загрозами. Саме здатність системи публічного управління швидко навчатися та законодавчо закріплювати уроки цієї війни визначатиме життєздатність держави в нову цифрову епоху.

ВИСНОВКИ

У магістерській роботі успішно досягнуто поставленої мети та в повному обсязі вирішено визначені завдання, що дозволило здійснити комплексний аналіз системи публічного управління процесами використання інформаційних технологій у сфері національної безпеки України. Логіка дослідження дала змогу послідовно пройти шлях від теоретичного осмислення трансформації безпекової парадигми та оцінки реального стану цифрових інструментів в умовах війни до вивчення передового міжнародного досвіду та розробки стратегічних рекомендацій. Отримані результати підтверджують, що інтеграція сучасних технологій у сектор безпеки вимагає не лише технічного переозброєння, а й фундаментальних змін в управлінських підходах, нормативному регулюванні та кадровій політиці держави.

1. Розкрито теоретичні засади використання інформаційних технологій у сфері безпеки та виокремлено трансформацію підходів від традиційного кіберзахисту до парадигми кіберстійкості та екосистемного управління. Встановлено, що в умовах гібридних загроз інформаційні технології еволюціонували з допоміжного адміністративного інструментарію в самостійне середовище реалізації державної політики та ведення бойових дій. Доведено, що сучасна теорія публічного управління зміщує фокус з концепції «абсолютного зкіберахисту» на концепцію «кіберстійкості», яка визначає ефективність системи не відсутністю інцидентів, а здатністю державних інституцій адаптуватися до перманентного деструктивного впливу та швидко відновлювати функціональність.

Цей теоретичний зсув обґрунтовує необхідність переходу до мережецентричної моделі управління, де держава більше не є монополістом у сфері безпеки, а виступає координатором складної екосистеми. Така модель передбачає залучення широкого кола стейкхолдерів – від приватних IT-компаній до волонтерських спільнот («білих хакерів»), що трансформує

громадянина з пасивного об’єкта захисту на активного суб’єкта забезпечення національної безпеки через механізми цифрового спротиву та стратегічних комунікацій.

2. Проаналізовано чинне нормативно-правове забезпечення та інституційну структуру управління національною безпекою в ІТ-сфері, зокрема в контексті гармонізації українського законодавства з європейською директивою NIS2. Виявлено, що національна система управління є поліцентричною та базується на розподіленій відповідальності, де Мінцифра виступає архітектором інновацій, а силові відомства забезпечують захист периметра. Водночас констатовано, що чинне законодавство містить прогалини щодо захисту критичної інфраструктури в умовах війни та спирається на застарілі стандарти сертифікації.

Обґрунтовано, що повноцінна імплементація Директиви NIS2 є безальтернативним кроком для інтеграції України в Єдиний цифровий ринок ЄС. Цей процес вимагає не просто технічних змін, а фундаментальної перебудови управлінської культури: переходу від сприйняття кібербезпеки як суто технічної проблеми до її розуміння як стратегічного ризику, за який несе персональну відповідальність вище керівництво. Також наголошено на необхідності посилення контролю за безпекою ланцюгів постачання, що є критичним для стійкості всієї екосистеми.

3. Оцінено поточний стан впровадження цифрових інструментів (системи Delta, екосистеми Brave1, цифрової мобілізації) у діяльність сектору безпеки і оборони України та виявлено ключові управлінські та технічні проблеми. Встановлено, що сектор безпеки здійснив якісний стрибок від «паперової армії» до елементів мережецентричної війни, де системи ситуаційної обізнаності (Delta) та платформи оборонних інновацій (Brave1) забезпечують технологічну перевагу та пришвидшення циклу прийняття рішень. Однак цей процес характеризується станом «адаптивного хаосу», де державні регуляції часто не встигають за темпами розвитку технологій «на землі».

Виявлено критичні проблеми фрагментації інформаційного простору («зоопарк технологій»), що проявляється у відсутності повної інтероперабельності між державними та волонтерськими системами і призводить до необхідності ручного перенесення даних. Акцентовано увагу на неефективності чинної моделі кадрового забезпечення: механізми бронювання не враховують специфіку ІТ-ринку, що створює загрозу втрати унікального інтелектуального ресурсу. Також ідентифіковано ризики «тіньової цифровізації», коли управління військами фактично здійснюється через обладнання, яке юридично не стоїть на балансі держави.

4. Узагальнено передовий міжнародний досвід США, Ізраїлю та Естонії щодо побудови моделей цифрової оборони та визначено можливості його адаптації до українських реалій. Доведено, що успішні національні моделі базуються не на жорсткій централізації, а на культурі довіри та партнерства: між державою та приватним сектором (модель CISA у США), між армією та інноваційною екосистемою (модель «Talpiot» в Ізраїлі) та між урядом і громадянським суспільством (модель «Кіберліги» в Естонії).

На основі цього досвіду запропоновано конкретні механізми адаптації для України: трансформацію кластеру Brave1 у повноцінну державну інституцію оборонних інновацій, що дозволить системно фінансувати R&D; впровадження концепції «цифрових посольств» для юридичного захисту державного суверенітету в хмарному середовищі; а також зміну філософії комплектування майбутніх Кіберсил з акцентом на «управління талантами», а не на стандартні мобілізаційні процедури.

5. Обґрунтовано стратегічні напрями оптимізації державної політики, фокусуючись на нових підходах до фінансування оборонних інновацій, кадрового забезпечення та створення «цифрових посольств». Доведено, що для переходу від тактичного реагування до стратегічного розвитку держава має створити умови для залучення приватного венчурного капіталу в сектор оборонних технологій та запровадити прозорі механізми страхування воєнних ризиків для інвесторів. Запропоновано лібералізувати систему експортного

контролю, дозволивши продаж окремих технологій союзникам, що дасть змогу українським компаніям отримувати валютну виручку для реінвестування у власні R&D.

Визначено, що забезпечення цифрового суверенітету вимагає не просто використання хмарних технологій, а ініціювання підписання міжурядових угод про створення «цифрових посольств», які нададуть українським реєстрам за кордоном дипломатичний імунітет. У кадровій сфері аргументовано необхідність відмови від застарілих підходів до мобілізації на користь диференційованої системи, яка дозволяє ефективно використовувати потенціал цивільних інженерів для вирішення завдань кіберзахисту та радіоелектронної боротьби.

6. Розроблено шляхи вдосконалення організаційно-правового механізму, зокрема щодо захисту прав інтелектуальної власності у сфері оборонних технологій та переходу до ризик-орієнтованих стандартів сертифікації замість застарілих систем захисту. Запропоновано запровадження спеціального правового режиму для оборонних технологій, який базується на моделі Урядових цільових правах: майнові права на розробку залишаються за винахідником, що дозволяє залучати інвестиції та масштабувати бізнес, а держава отримує безвідкличну безоплатну ліцензію на використання продукту для потреб оборони.

Обґрунтовано необхідність дерегуляції у сфері технічного захисту інформації шляхом відмови від тотального застосування статичної Комплексної системи захисту інформації для систем, що не обробляють державну таємницю. Натомість запропоновано перехід до декларування відповідності міжнародним стандартам (ISO/IEC 27001, NIST) та впровадження процедур постійного моніторингу ризиків, що значно пришвидшить розгортання ІТ-систем. Також наголошено на важливості гармонізації національних грифів секретності зі стандартами НАТО та законодавчого визнання програмного забезпечення повноцінним оборонним активом, що спростить процедури його обліку, списання та модернізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 10 запитань про «Оберіг»: хто матиме доступ до даних і як їх верифікуватимуть / *DOU*. 2024. URL: https://dou.ua/lenta/interviews/register-oberig-blitz (дата звернення: 07.12.2025).

2. Challenges in Protecting and Restoring Critical Infrastructure Through Private Sector Engagement. *Business Ombudsman Council*. 2025. URL: https://boi.org.ua/wp-content/uploads/2025/03/challenges-in-protecting-and-restoring-critical-infrastructure-through-private-sector-engagement.pdf (last accessed: 07.12.2025).

3. Crandall M. Understanding Estonia's Cyber Support for Ukraine: Building Resilience, Not Status. *Applied Cybersecurity & Internet Governance*. 2024. Vol. 3. No 1. P. 78–90. https://doi.org/10.60097/ACIG/190396 (last accessed: 07.12.2025).

4. Cyber command: defending a digital society / *e-Estonia*. 2025. URL: https://e-estonia.com/cyber-command-defending-a-digital-society (last accessed: 07.12.2025).

5. Cyber Governance for Boards. *The National Cyber Security Centre*. URL: https://www.ncsc.gov.uk/cyber-governance-for-boards/overview (last accessed: 07.12.2025).

6. Fact Sheet: Cisa Leads Call For Strengthening National Cybersecurity. *Critical Infrastructure Security Agency*. URL: https://www.cisa.gov/sites/default/files/publications/CISA_Cybersecurity_Resources_Fact_Sheet_508c.pdf (last accessed: 07.12.2025).

7. From Continuity to Culture? Preserving and Securing Ukrainian Public and Private Sector Data / *ComplexDiscovery OÜ*. URL: https://complexdiscovery.com/from-continuity-to-culture-preserving-and-securing-ukrainian-public-and-private-sector-data (last accessed: 07.12.2025).

8. Greene J. United in Cyber Defense: A Model for Operational

Collaboration. *Critical Infrastructure Security Agency*. 2025. URL: https://www.cisa.gov/news-events/news/united-cyber-defense-model-operational-collaboration (last accessed: 07.12.2025).

9. Heilweil Rebecca. DHS watchdog finds mismanagement in critical cyber talent program / *FedScoop*. 2025. URL: https://fedscoop.com/cisa-cyber-incentive-program-dhs-inspector-general-report (last accessed: 07.12.2025).

10. Holm P. Estonia's bold approach to cyber security: a holistic model for Europe. *e-Estonia*. 2025. URL: https://e-estonia.com/estonias-cyber-security-model-for-europe (last accessed: 07.12.2025).

11. Israel – National Cyber Directorate (INCD). *Cybil*. URL: https://cybilportal.org/actors/cyber-israel-national-cyber-directorate (last accessed: 07.12.2025).

12. Israel Cybersecurity Strategy 2025: A Strategic Gateway for U.S. *International Trade Administration*. 2025. URL: https://www.trade.gov/market-intelligence/israel-cybersecurity-strategy-2025-strategic-gateway-us (last accessed: 07.12.2025).

13. Key Data & Cybersecurity Laws / *Baker McKenzie's Resource Hub*. URL: https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/emea/israel/topics/key-data-and-cybersecurity-laws (last accessed: 07.12.2025).

14. Manuel Rojoef. Ukraine Records Cyberattack on Armed Forces, Defense Enterprises / *The Defense Post*. 2024. URL: https://thedefensepost.com/2024/12/10/ukraine-cyberattack-armed-forces (last accessed: 07.12.2025).

15. Melkozerova Veronika. Ukraine's army digitization law sparks worries over data protection / *Politico Pro*. 2024. URL: https://subscriber.politicopro.com/article/2024/01/ukraines-army-digitization-law-sparks-worries-over-data-protection-00135796 (last accessed: 07.12.2025).

16. Murdoch Benjamin. NATO wants Ukraine's combat-tested innovations – and is putting €10 million behind them / *Euromaidan Press*. 2025. URL: https://euromaidanpress.com/2025/11/27/ukraine-and-nato-launch-unite-brave-nato

(last accessed: 07.12.2025).

17. National Cyber Strategy 2022 Annual Progress Report 2022-2023. *Cabinet Office*. 2023. URL: https://www.gov.uk/government/publications/national-cyber-strategy-2022-annual-progress-report-2022-2023/national-cyber-strategy-2022-annual-progress-report-2022-2023-html (last accessed: 07.12.2025).

18. NATO and Ukraine – Successes and Complexities on the Path to Interoperability / *NATO C2COE*. 2024. URL: https://c2coe.org/download/nato-and-ukraine-successes-and-complexities-on-the-path-to-interoperability (last accessed: 07.12.2025).

19. NATO Centres of Excellence – Cooperative Cyber Defence (CCD COE) / *NATO*. URL: https://www.act.nato.int/article/nato-centres-of-excellence-cooperative-cyber-defence-ccd-coe (last accessed: 07.12.2025).

20. NATO Develops a Cloud Infrastructure for Ukraine's Classified Battle Data / *DEFCROS News*. URL: https://news.defcros.com/nato-develops-cloud-infrastructure-for-ukraine (last accessed: 07.12.2025).

21. Or-Hof D. Space Law 2025. *Chambers and Partners*. 2025. URL: https://practiceguides.chambers.com/practice-guides/comparison/1224/16768/26014-26015-26016-26017-26018-26019-26020-26021-26022 (last accessed: 07.12.2025).

22. PwC провела бізнес-сніданок під час Brave1 Defense Tech Valley саміту / PwC Україна. URL: https://www.pwc.com/ua/en/press-room/2025/pwc-business-breakfast-brave1-defense-tech-summit.html (дата звернення: 07.12.2025).

23. Review of cybersecurity news in Ukraine, tendencies, and world events related to the First World Cyber War / *RNBO*. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20240916/2024%2008%20Cyber%20digest_ENG.pdf (last accessed: 07.12.2025).

24. Schwennesen P. Eyewitness to War: Ukraine's tech hubs and digital Darwinism. *GIS Reports*. 2025. URL: https://www.gisreportsonline.com/r/ukraine-digital-darwinism (last accessed: 07.12.2025).

25. Serhiienko N. Information Security as a Fundamental Component of National Security. *Administrative Law and Process*. 2023. No 9.

https://doi.org/10.32849/2663-5313/2023.9.05 (last accessed: 07.12.2025).

26. Sokiran M. Basic Principles of Public Administration of Critical Information Infrastructure: the Example of Ukraine. *Advanced Space Law*. 2021. Vol. 7. P. 63–72. https://doi.org/10.29202/asl/7/7 (last accessed: 07.12.2025).

27. Talpiot program / *Wikipedia*. URL: https://en.wikipedia.org/wiki/Talpiot_program (last accessed: 07.12.2025).

28. The Accountant General at the Ministry of Finance, in cooperation with the Directorate of Defense Research & Development (DDR&D), appealed to the Knesset Finance Committee to receive approval for providing a state guarantee for the purpose of establishing / Ministry of Finance. URL: https://www.gov.il/en/pages/press_10092025 (last accessed: 07.12.2025).

29. The Israeli Tech Ecosystem / *Israel Innovation Authority*. URL: https://innovationisrael.org.il/en/israeli-tech-ecosystem (last accessed: 07.12.2025).

30. Ukraine-US Cybersecurity Activity in Ukraine. *DAI*. URL: https://www.dai.com/our-work/projects/ukraine-cybersecurity-for-critical-infrastructure-activity (last accessed: 07.12.2025).

31. United States and Ukraine Expand Cooperation on Cybersecurity. *Critical Infrastructure Security Agency*. 2022. URL: https://www.cisa.gov/news-events/news/united-states-and-ukraine-expand-cooperation-cybersecurity (last accessed: 07.12.2025).

32. Unna I. Success Story: Israel National Cyber Directorate Version 2.0. *National Institute of Standards and Technology*. URL: https://www.nist.gov/cyberframework/success-stories/israel-national-cyber-directorate-version-20 (last accessed: 07.12.2025).

33. Аналітична записка з питань порівняльного законодавства Європейського Союзу, держав-членів ЄС та інших держав щодо забезпечення кібербезпеки / Дослідницька служба Верховної Ради України. URL: https://research.rada.gov.ua/uploads/documents/32612.pdf (дата звернення: 07.12.2025).

34. Бадрак В., Габідулін І. Вкрадені мізки, або як Україні зупинити

витік інновацій під час війни. *Еспресо*. 2025. URL: https://espreso.tv/article-vkradeni-mizki-abo-yak-ukraini-zupiniti-vitik-innovatsiy-pid-chas-viyni (дата звернення: 07.12.2025).

35. В Україні запустили defense tech cluster BRAVE1, який стимулюватиме розвиток військових інновацій та оборонних технологій. *Міністерство цифрової трансформації України*. 2023. URL: https://thedigital.gov.ua/news/technologies/v-ukraini-zapustili-defense-tech-cluster-brave1-yakiy-stimulyuvatime-rozvitok-viyskovikh-innovatsiy-ta-oboronnikh-tekhnologiy (дата звернення: 07.12.2025).

36. Величко Л., Білоконь М. Гібридні загрози транспортній інфраструктурі: виклики для державного регулювання та національної безпеки. *Теорія та практика державного управління*. 2024. № 2(79). С. 442–464. https://doi.org/10.26565/1727-6667-2024-2-23 (дата звернення: 07.12.2025).

37. Вплив Директиви NIS2 на підприємства критичної інфраструктури України в межах інтеграції до ЄС. *Deloitte*. 2025. URL: https://www.deloitte.com/ua/uk/services/consulting/perspectives/impact-of-nis2-directive-on-ukraine-critical-infrastructure-enterprises-eu-integration.html (дата звернення: 07.12.2025).

38. Впровадження цифрових технологій та боротьба з корупцією. НАБУ та Мінцифри підписали меморандум / *Національне антикорупційне бюро України*. 2023. URL: https://nabu.gov.ua/news/vprovadzhennia-tcifrovikh-tekhnolog-i-ta-borot-ba-z-koruptc-iu-nabu-ta-m-ntcifri-p-dpisali-memorandum (дата звернення: 07.12.2025).

39. Директива ЄС NIS2: що це таке, для яких потреб розроблена та для чого Україна її імплементує. *Державна служба спеціального зв'язку та захисту інформації України*. 2025. URL: https://cip.gov.ua/ua/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye (дата звернення: 07.12.2025).

40. ДОТ Міноборони успішно пройшов незалежний фінансовий аудит / *Міністерство оборони України*. 2025. URL: https://mod.gov.ua/news/

dot-minoboroni-uspishno-projshov-nezalezhnij-finansovij-audit (дата звернення: 07.12.2025).

41. Звіт Рахункової палати за 2024 рік / *Рахункова палата*. URL: https://rp.gov.ua/upload-files/Activity/Reports/2024/ZVIT_RP_2024.pdf (дата звернення: 07.12.2025).

42. Зіменков С. Кібербезпека на міжнародному рівні: Виклики та можливості NIS2 для українських компаній. *International Advisers Association*. 2024. URL: https://iaa.international/publication/kiberbezpeka-na-mizhnarodnomu-rivni-vikliki-ta-mozhlivosti-nis2-dlia-ukrainskikh-kompanii (дата звернення: 07.12.2025).

43. Кабачинський І. Brave1 запустив Brave1 Club – спрощена процедура вступу до кластера. *Scroll*. 2025. URL: https://scroll.media/2025/06/12/brave1-zapustyv-brave1-club (дата звернення: 07.12.2025).

44. Кропива та DELTA: технології, що змінюють підхід до війни / *Національна академія Національної гвардії України*. 2025. URL: https://nangu.edu.ua/news/kropiva-ta-delta-tehnologii-tsho-zminyuyut-pidhid-do-vijni (дата звернення: 07.12.2025).

45. Кукін І. В. Комплексний механізм публічного управління інформаційною безпекою особистості у сфері національної безпеки та її прикордонному секторі. *Публічне управління та митне адміністрування*. 2020. № 4 (27). С. 134–139. DOI: https://doi.org/10.32836/2310-9653-2020-4.21.

46. Мазник Л. В., Двуліт З. П. Управління діяльністю фахівців з кібербезпеки в умовах повномасштабного вторгнення. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку*. 2023. № 2. С. 9. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2023/dec/32677/menedzhment223maket-54-65.pdf (дата звернення: 07.12.2025).

47. Мануйлов Є. М., Калиновський Ю. Ю. Інформаційний суверенітет України: сучасні виклики та загрози духовній сфері. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2019. № 3(42). С. 22–33. https://doi.org/10.21564/2075-7190.42.170288 (дата

звернення: 07.12.2025).

48. Міноборони та Мінцифри створюють єдину екосистему підтримки українських виробників зброї / *Міністерство оборони України*. 2025. URL: https://mod.gov.ua/news/minoboroni-ta-minczifri-stvoryuyut-yedinu-ekosistemu-pidtrimki-ukrayinskih-virobnikiv-zbroyi (дата звернення: 07.12.2025).

49. Мінцифри презентувало стратегію розвитку електронних комунікацій до 2030: долучайтеся до обговорення / *Урядовий портал*. 2024. URL: https://www.kmu.gov.ua/news/mintsyfry-prezentuvala-stratehiiu-rozvytku-elektronnykh-komunikatsii-do-2030-doluchaitesia-do-obhovorennia (дата звернення: 07.12.2025).

50. НАТО і Україна анонсували нову спільну ініціативу з прискорення оборонних інновацій: «UNITE – Хоробра НАТО» / НАТО. 2025. URL: https://www.nato.int/en/news-and-events/articles/news/2025/11/26/nato-and-ukraine-announce-new-joint-initiative-to-accelerate-defence-innovation-unite-brave-nato?selectedLocale=uk (дата звернення: 07.12.2025).

51. Недашківська Юлія. ФОПам тут не місце: Як забронювати ІТ-фахівця від мобілізації / *Цензор*. 2023. URL: https://censor.net/biz/resonance/3407098/fopam_tut_ne_mistse_yak_zabronyuvaty_itfahivtsya_vid_mobilizatsiyi (дата звернення: 07.12.2025).

52. Орлов О., Дворянов В. Гібридні загрози у цифрову добу: шляхи підвищення ефективності державних механізмів протидії. *Науково-освітній інноваційний центр суспільних трансформацій*. 2025. https://doi.org/10.54929/monograph-11-2025-03-01 (дата звернення: 07.12.2025).

53. Оцінка стану розвитку національної системи кібребезпеки. Аналіз за результатами онлайн опитування. *Рада національної безпеки та оборони України*. Київ, 2021. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/analityka_1.pdf (дата звернення: 07.12.2025).

54. Позиція щодо закупівельних агенцій та рекомендацій Огляду НАТО / Армія PRO. 2024. URL: https://www.army-pro.com/pozycziya-shhodo-zakupivelnyh-agenczij-ta-rekomendaczij-oglyadu-nato (дата звернення:

07.12.2025).

55. Положення про Міністерство цифрової трансформації України : постанова Кабінету Міністрів України від 18 вересня 2019 р. № 856. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF (дата звернення: 07.12.2025).

56. Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки / Рада національної безпеки та оборони України. URL: https://www.rnbo.gov.ua/files/2022/NKCK/%D0%9F%D0%BE%D1%80%D1%8F%D0%B4%D0%BE%D0%BA_%D0%B2%D0%B7%D0%B0%D1%94%D0%BC%D0%BE%D0%B4%D1%96%D1%97.pdf (дата звернення: 07.12.2025).

57. Правовий аналіз проекту концепції інформаційної безпеки України. *Організація з безпеки та співробітництва в Європі. Бюро Представника ОБСЕ з питань свободи ЗМІ*. 2015. URL: https://www.osce.org/sites/default/files/f/documents/9/9/175046.pdf (дата звернення: 07.12.2025).

58. Про затвердження стандарту вищої освіти за спеціальністю 281 «Публічне управління та адміністрування» для другого (магістерського) рівня вищої освіти. Наказ МОН № 1001 від 04.08.2020 року / Міністерство освіти і науки України. URL: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2020/08/05/281publichne-upravlinnya-ta-administruvannya-magistr.pdf (дата звернення: 07.12.2025).

59. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради (ВВР)*. 2017. № 45. Ст. 403. https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 07.12.2025).

60. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради (ВВР)*. 2017. № 45. Ст. 403. https://zakon.rada.gov.ua/laws/show/2163-VIII#Text (дата звернення: 07.12.2025).

61. Про прийняття за основу проекту Закону України про Кіберсили

Збройних Сил України. Документ 4628-IX, прийняття від 09.10.2025 / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/4628-IX#Text (дата звернення: 07.12.2025).

62. Проект зміцнення управління державними ресурсами частини b «Підтримка впровадження стратегії управління державними фінансами» (порядковий номер проекту p161586) / Міністерство фінансів України. URL: https://mof.gov.ua/storage/files/IC-MF-15_REoI.pdf (дата звернення: 07.12.2025).

63. Рівень захисту IP в Україні: закони є, але бракує правозастосування / Національна асоціація адвокатів України. 2025. URL: https://unba.org.ua/news/10795-riven-zahistu-ip-v-ukraini-zakoni-e-ale-brakue-pravo zastosuvannya.html (дата звернення: 07.12.2025).

64. Сертифікація ISO: практика Органу оскарження / ProZorro. 2021. URL: https://infobox.prozorro.org/articles/sertifikaciya-iso-praktika-organu-oskarzhennya (дата звернення: 07.12.2025).

65. Спільний пресреліз: ЄС та Україна посилюють розробку рішень для ведення бойових дій за допомогою «BraveTech EU» / Європейська Комісія. 2025. URL: https://ec.europa.eu/commission/presscorner/detail/uk/ip_25_1794 (дата звернення: 07.12.2025).

66. Указ Президента України Про Національний координаційний центр кібербезпеки. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 07.12.2025).

67. Урсол О. Теоретичні основи і розвитку публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України. *Honor and Law*. 2025. № 2(93). С. 152–159. https://doi.org/10.33405/2078-7480/2025/2/93/339411 (дата звернення: 07.12.2025).

68. Шинко А. Мінцифри забирає повноваження у Держспецзв'язку. *Ukrainian Military Pages*. 2023. https://www.ukrmilitary.com/2023/07/dsszzi-mintcyfry.html (дата звернення: 07.12.2025).

69. Що робити якщо немає в реєстрі Оберіг? / *ТОВ «ЮРИДИЧНА КОМПАНІЯ ІНСЕІНІН»*. URL: https://inseinin.com.ua/tpost/bolh3c9r21-scho-

robiti-yakscho-nema-v-restr-oberg (дата звернення: 07.12.2025).

70. Що таке система DELTA і як вона задає тренди для країн НАТО? / *Міністерство оборони України*. 2024. URL: https://mod.gov.ua/news/shho-take-sistema-delta-i-yak-vona-zadae-trendi (дата звернення: 07.12.2025).

71. Що таке система DELTA і як вона задає тренди для країн НАТО? *Міністерство оборони України*. 2024. https://mod.gov.ua/news/shho-take-sistema-delta-i-yak-vona-zadae-trendi (дата звернення: 07.12.2025).

72. Щодо обстановки в сфері кібер на 23-24 лютого 2024 року / *CERT-UA*. 2024. URL: https://cert.gov.ua/article/6277822 (дата звернення: 07.12.2025).

73. Ярова М. 4 критичні помилки стартапів у сфері інтелектуальної власності і як їх уникнути. *Scroll*. 2025. URL: https://scroll.media/2025/11/05/iv-startapiv (дата звернення: 07.12.2025).